Microsoft® System Center Data Protection Manager 2006

Betriebshandbuch

Microsoft

Informationen in diesem Dokument, einschließlich URLs und anderen Verweisen auf Internetseiten, können ohne vorherige Ankündigung geändert werden. Sofern nichts anderes angegeben ist, sind die in den Beispielen genannten Unternehmen, Organisationen, Produkte, Domänennamen, E-Mail-Adressen, Logos, Personen, Orte und Ereignisse frei erfunden. Jede Ähnlichkeit mit tatsächlichen Unternehmen, Organisationen, Produkten, Domänennamen, E-Mail-Adressen, Logos, Personen, Orten oder Ereignissen ist rein zufällig. Die Benutzer/innen sind verpflichtet, sich an alle anwendbaren Urheberrechtsgesetze zu halten. Unabhängig von der

Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen, usw.) dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von Microsoft eingeräumt.

© 2005 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, MS-DOS, Windows, Windows NT, Windows Server und Active Directory sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Inhalt

Verwenden dieses Handbuchs 1
Über das Betriebshandbuch von DPM 2006 1
Zielgruppe 1
Umfang 1
Inhalt 2
Dokumentkonventionen 2
Namenskonventionen 3
Konventionen für Leserhinweise 3
Formatierungskonventionen 4
Andere DPM-Dokumentationen 4
Andere DPM-Dokumentationen 4
Produktsupportinformationen 6

Kapitel 1: Funktionen von Data Protection Manager: Übersicht 7
DPM-Bereitstellung bei Northwind Traders 7
Überwachen von DPM-Vorgängen 9
Verwenden von DPM zum Wiederherstellen von Daten 10
Überwachen der Leistung von DPM 11
Warten von DPM-Servern und Dateiservern 12
Archivieren von DPM für die Notfall-Wiederherstellung 13
Beheben von Fehlern in DPM-Vorgängen 13

Kapitel 2: Überwachen von Data Protection Manager 13
Einrichten eines Überwachungszeitplans 16
Suchen nach Informationen 17
Überwachungsmethoden 18
DPM-Verwaltungskonsole 18
Aufgabenbereich **Überwachung**: **Warnungen** 19
Aufgabenbereich **Überwachung**: **Aufträge** 20
Aufgabenbereich **Schutz von Daten** 20

Aufgabenbereich **Verwaltung**: **Datenträger** 21
Aufgabenbereich **Verwaltung**: **Agents** 21
Aufgabenbereich **Berichterstellung** 22
Berichte und Benachrichtigungen über Warnungen in E-Mails 25
DPM Management Pack 26

Kapitel 3: Verwalten der Leistung 25
Auswirkungen von DPM-Vorgängen auf die Leistung 30
Replikaterstellung 30
Nachverfolgung von Änderungen 31
Synchronisierung 31
Konsistenzprüfung 32
DPM-Prozesse 32
Erfassen von Leistungsdaten 33
Leistungsindikatoren 33
Netzwerkverkehrbericht 36
Verbessern der Leistung 37
Ermitteln maximaler Auslastungen 37
Ändern von Auslastungen 39
Verwenden der Bandbreitenbeschränkung für das Netzwerk 39
Verwenden der Komprimierung über das Netzwerk 41
Staffeln von Startzeiten für die Synchronisierung 41
Planen von Synchronisierungsaufträgen 42
Planen von Konsistenzprüfungen 42
Manuelles Erstellen von Replikaten 43
Erhöhen der Kapazität 44
Verwalten der Leistung von DPM in einem WAN 44

Kapitel 4: Verwalten von Servern 41
Durchführen allgemeiner Serverwartung 46
Verwenden von Windows-Wartungstools 46
Aktualisieren des Betriebssystems 47
Ausführen von Antivirusprogrammen 48
Sichern von Servern 49
Verwalten des DPM-Servers 50
Suchen von DPM-Servern in Active Directory 50
Hinzufügen von Datenträgern zum DPM-Server 51
Verschieben des DPM-Servers zwischen Domänen 52
Ändern der Zeitzone des DPM-Servers 52
Neu starten des DPM-Servers 53
Verwalten von Dateiservern 54
Verschieben von Dateiservern zwischen Domänen 54
Umbenennen eines Dateiservers 55
Wiederherstellen des Schutzes auf einem Dateiserver nach Laufwerkfehler oder Datenträgeraktualisierung 55
Ausführen von Bildschirmschonern auf Dateiservern 57
Ändern der Zeitzone von Dateiservern 57
Koordinieren des Schutzes zwischen Zeitzonen 58
Zeitanzeige in DPM 58
Planen der ersten Replikaterstellung 58
Sommer-/Winterzeit in DPM 59
Konfigurieren von Firewalls 59
Protokolle und Ports 59
Wann ein Konfigurieren der Firewall erforderlich ist 61
Konfigurieren einer Firewall auf einem DPM-Server 61
Konfigurieren einer Firewall auf einem Dateiserver 61

Kapitel 5: Archivieren und Wiederherstellen von Daten 59
Planen der Archivierung und Wiederherstellung von Daten 64
Ermitteln der Sicherungskomponenten 65
Planen von Sicherungen 65
Auswählen von Sicherungssoftware 66
Sicherungssoftware, die DPM unterstützt 66
Sicherungssoftware, die VSS unterstützt 67
Sicherungssoftware, die VSS nicht unterstützt 67
Sicherungstools in DPM 67
Integrieren von DPM in eine Sicherungstopologie 68
Sichern von Servern 69
Archivieren von Datenbanken und Replikaten 70
Verwenden von Sicherungssoftware, die DPM unterstützt 70
Verwenden von Sicherungssoftware, die VSS unterstützt 71
Verwenden von Sicherungssoftware, die VSS nicht unterstützt 72
Verwenden von DpmBackup zum Erstellen von Sicherungsschattenkopien 72
DpmBackup-Syntax 74
Verwenden von DpmBackup mit Bereitstellungspunkten 74
Wiederherstellen von Daten vom Band auf Dateiserver 75
Verwenden von FsPathMerge zum Reparieren von Pfaden auf Dateiservern 76
FsPathMerge-Syntax 76
Parameter 76
Beispiel 77
Wiederherstellen eines DPM-Servers 78
Wiederherstellen von Datenbanken 78
Verwenden von DpmSync zum Wiederherstellen von Datenbanken 78
DpmSync-Syntax 78
Wiederherstellen von Replikaten 80
Verwenden von DpmPathMerge zum Reparieren von Pfaden 81
DpmPathMerge-Syntax 81
Verwenden von FsPathMerge zum Reparieren von Pfaden auf einem DPM-Server 82
Wiederherstellen eines DPM-Servers auf einem neuen Computer 83

Kapitel 6: Problembehandlung 81
Standardverfahren zur Problembehandlung 86
Überprüfen des Status des DPM-Diensts 86
Überprüfen der Namensauflösung 87
Erkennen von DNS-Fehlern 88
Weitere Ressourcen 89
Tools 89
Beheben von „Zugriff verweigert“-Fehlern 89
Behandeln von Problemen bei der DPM-Installation 90
Behandeln von Problemen bei der Installation des Datei-Agents 92
Behandeln von Problemen beim Schutz von Daten 98
Behandeln von allgemeinen Problemen beim Schutz von Daten 98
Behandeln von Problemen beim manuellen Erstellen von Replikaten 103
Behandeln von Datenwiederherstellungsproblemen 105
Behandeln von allgemeinen Datenwiederherstellungsproblemen 105
Behandeln von Problemen beim Konfigurieren der Endbenutzerwiederherstellung 106
Behandeln von Problemen bei der Endbenutzerwiederherstellung 107
Behandeln von Problemen bei der Endbenutzerwiederherstellung und DFS 110
Behandeln von Problemen bei der Berichterstellung 111
Behandeln von Leistungsproblemen 120
Behandeln von Problemen bei ungenügendem Arbeitsspeicher 121
So erhalten Sie weitere Informationen zu ungenügendem Arbeitsspeicher 121

Behandeln von Problemen mit der CPU-Auslastung....122
So erhalten Sie weitere Informationen zur CPU-Auslastung....122
Behandeln von Problemen mit der Warteschlangenlänge des Datenträgers....123
So erhalten Sie weitere Informationen zur Leistung von Datenträgerressourcen....123
Behandeln von Datenbankproblemen....124
Weitere Ressourcen für die Datenbankproblembehandlung....129
Behandeln von Problemen beim Archivieren und Wiederherstellen von DPM....130
Behandeln von Problemen mit DpmBackup und DPM Writer....130
Behandeln von Problemen mit FsPathMerge....136
Behandeln von Problemen mit DpmPathMerge....139

Anhang A: Fehlercodes in Data Protection Manager 2006....137

Anhang B: Schemaerweiterungen in Data Protection Manager 2006....141
Von DPM hinzugefügte Klassen....147
Von DPM hinzugefügte Attribute....148
Das Attribut „ms-BackupSrv-Share“....148
Das Attribut „ms-ProductionSrv-Share“....149

Verwenden dieses Handbuchs

Willkommen beim Betriebshandbuch von Microsoft System Center Data Protection Manager 2006. In diesem Handbuch werden Vorgänge in Microsoft System Center Data Protection Manager 2006 (DPM) erläutert und eine Problembehandlungsanleitung für das Produkt bereitgestellt.

Die in den Beispielen genannten Unternehmen, Organisationen, Produkte, Domänennamen, E-Mail-Adressen, Logos, Personen, Orte und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit tatsächlichen Unternehmen, Organisationen, Produkten, Domänennamen, E-Mail-Adressen, Logos, Personen, Orten oder Ereignissen ist rein zufällig.

In diesem Kapitel

Über das Betriebshandbuch von DPM 2006

Dokumentkonventionen

Andere DPM-Dokumentationen

Produktsupportinformationen

Über das Betriebshandbuch von DPM 2006

Das Betriebshandbuch von DPM 2006 steht auf der Technet-Website Data Protection Manager (http://go.microsoft.com/fwlink/?LinkId=46363) zur Verfügung.

Zielgruppe

Die Hauptzielgruppe für das Betriebshandbuch von DPM 2006 besteht aus IT-Administratoren, die Verwaltung, Wartung und Problembehandlung von Data Protection Manager durchführen. Dieses Handbuch soll sowohl IT-Neulinge als auch erfahrene IT-Administratoren bei der Wartung von DPM in ihrer Organisation unterstützen. Es wird vorausgesetzt, dass der Leser bereits mit der DPM-Verwaltungskonsole und den im Planungs- und Bereitstellungshandbuch von Microsoft Data Protection Manager 2006 beschriebenen Konfigurationsaufgaben vertraut ist.

Umfang

In diesem Handbuch finden Administratoren Informationen zur Überwachung von DPM, dem Verwalten der Auswirkungen von Vorgängen zum Schutz von Daten auf die Netzwerkleistung, der Behandlung von Warnungen, Berichten und Ressourcenwarnungen, der Wiederherstellung von Daten, der Archivierung und Wiederherstellung von Daten auf DPM-Servern und Dateiservern sowie der Behandlung der häufigsten Probleme. Das Betriebshandbuch von DPM 2006 stellt Administratoren Informationen zur Verfügung, die sie zum Verwalten noch andauernder Vorgänge zum Schutz von Daten ebenso benötigen wie zum Beheben von Problemen beim Schutz von Daten, der Leistung und der Wiederherstellung.

Eine Beschreibung von Themen, die in anderen DPM-Dokumentationen behandelt werden, finden Sie weiter unten in diesem Abschnitt unter „Andere DPM-Dokumentationen“.

Inhalt

Das Betriebshandbuch von DPM 2006 enthält die folgenden sechs Kapitel und zwei Anhänge:

- **Kapitel 1:** „Vorgänge in Data Protection Manager: Übersicht“ In diesem Kapitel wird eine Übersicht über die Vorgänge und Dokumentation von DPM bereitgestellt, indem die Erfahrungen eines Systemadministrators beschrieben werden, der für die Verwaltung und den Support von DPM verantwortlich ist.
- **Kapitel 2:** „Überwachen von Data Protection Manager“ In diesem Kapitel werden Empfehlungen für einen Überwachungszeitplan bereitgestellt und Methoden zum Überwachen und Erfassen von Informationen zu DPM-Vorgängen erläutert.
- **Kapitel 3:** „Verwalten der Leistung“ In diesem Kapitel werden die Auswirkungen von DPM-Prozessen auf Server- und Netzwerkleistung erläutert und Empfehlungen zur Leistungssteigerung bereitgestellt.
- **Kapitel 4:** „Verwalten von Servern“ In diesem Kapitel werden Richtlinien für die Serverwartung, Tipps zum Verwalten von DPM-Servern und Dateiservern, eine Beschreibung der Verwaltung von Zeitzonen durch DPM und eine Anleitung zum Konfigurieren von Firewalls bereitgestellt.
- **Kapitel 5:** „Archivieren und Wiederherstellen von Daten“ In diesem Kapitel wird erläutert, wie DPM-Replikate und DPM-Datenbanken archiviert und Daten im Notfall auf DPM- und Dateiservern wiederhergestellt werden.
- **Kapitel 6:** „Problembehandlung“ Dieses Kapitel enthält Vorgehensweisen zur allgemeinen Problembehandlung und zum Beheben spezifischer Fehler.
- **Anhang A:** „Fehlercodes in Data Protection Manager 2006“ In diesem Anhang wird der Zweck von Fehlermeldungen in DPM beschrieben. Für Informationen zur Fehlerbehebung wird auf das Kapitel „Problembehandlung“ verwiesen.

- **Anhang B:** „Schemaerweiterungen in Data Protection Manager 2006“ In diesem Anhang werden die Erweiterungen des Active Directory-Schemas beim Aktivieren der Endbenutzerwiederherstellung beschrieben.
- Glossar: An dieser Stelle werden Definitionen von Ausdrücken und Begriffen bereitgestellt, die für die Verwendung von DPM wichtig sind.

Dokumentkonventionen

In den folgenden Tabellen werden die Dokumentkonventionen beschrieben, die im Betriebshandbuch von DPM 2006 verwendet werden.

Benennungskonventionen

In der folgenden Tabelle werden die in diesem Handbuch verwendeten Benennungskonventionen aufgeführt.

Konvention	Beschreibung
Data Protection Manager DPM	Abkürzungen für Microsoft System Center Data Protection Manager 2006.
DPM-Agent-Koordinator Agent-Koordinator	Abkürzungen für Microsoft System Center Data Protection Manager 2006-Agent-Koordinator.
DPM-Datei-Agent Datei-Agent	Abkürzungen für Microsoft System Center Data Protection Manager 2006-Datei-Agent.
DPM Management Pack	Abkürzung für Microsoft System Center Data Protection Manager Management Pack.
SQL Server	Abkürzung für Microsoft SQL Server™ 2000.
SQL Server Reporting Services Reporting Services	Abkürzungen für Microsoft SQL Server™ 2000 Reporting Services.

Konventionen für Leserhinweise

Leserhinweise werden in diesem Handbuch verwendet, um auf zusätzliche und wichtige Informationen aufmerksam zu machen. In der folgenden Tabelle wird die Bedeutung der jeweiligen Hinweise erklärt.

Leserhinweis	Bedeutung
Reader Alert **Hinweis**	Hinweis auf zusätzliche Informationen, die nützlich für die Durchführung einer Aufgabe sind.
Wichtig	Hinweis auf zusätzliche Informationen, die wesentlich für die Durchführung einer Aufgabe sind.
Vorsicht	Hinweis auf möglichen Datenverlust, Sicherheitsrisiken oder andere schwerwiegendere Probleme.
Warnung	Warnung, dass die fehlerhafte oder unterlassene Ausführung eines bestimmten Vorgangs eine Fehlfunktion der Hardware oder Software zur Folge haben könnte.

Formatierungskonventionen

Die folgenden Formatierungskonventionen werden in diesem Handbuch verwendet.

Konvention	Beschreibung
Fettgedruckt	Wird für Benutzeroberflächenelemente, Beschriftungen in Menüs und Schaltflächen, Dialogfeldtitel und -optionen sowie für Symbol- und Menünamen verwendet.
Kursiv	Wird in Syntaxanweisungen oder Beschreibungen verwendet, um auf variable Namen oder Platzhalter hinzuweisen, für die vom Benutzer oder von DPM ein bestimmter Wert angegeben werden kann. Kursivschrift wird außerdem für neue Begriffe, Buchtitel und zur Hervorhebung verwendet.
`Festbreitenschrift`	Befehle und Syntax, die exakt wie angezeigt eingegeben werden müssen, werden in Festbreitenschriftart dargestellt.
Großbuchstaben	Tastaturbefehle werden in Großbuchstaben dargestellt.
Standardpfade	Speicherorte von Dateien und Ordnern werden als Standardpfadnamen festgelegt. Wenn für Installationen andere Speicherorte als die Standardpfade ausgewählt wurden, sollte der entsprechende Text in der Pfadangabe ersetzt werden.

Andere DPM-Dokumentationen

Andere DPM-Dokumentationen

Die DPM-Dokumentationen bieten Informationen zum Planen, Bereitstellen, Konfigurieren, Ausführen, Verwalten, Optimieren sowie zur Problembehandlung von DPM. Der größte Teil der Dokumentation ist im DPM-Produkt integriert. Die gesamte DPM-Dokumentation ist auch online verfügbar. In der folgenden Tabelle werden weitere Ressourcen in den DPM-Dokumentationen aufgeführt und ihr jeweiliger Inhalt beschrieben.

Ressource	Beschreibung
DPM-Hilfe	Die DPM-Hilfe bietet eine umfassende Themenauswahl, in der DPM-Grundbegriffe erklärt und Anleitungen zum Ausführen von Aufgaben mit DPM gegeben werden. Die DPM-Hilfe ist in DPM integriert und steht auch auf der Technet-Website Data Protection Manager (http://go.microsoft.com/fwlink/?linkid=46350) (in englischer Sprache) zur Verfügung.
Planungs- und Bereitstellungshandbuch von DPM 2006	Mit dem Planungs- und Bereitstellungshandbuch von DPM 2006 (http://go.microsoft.com/fwlink/?linkid=46351, in englischer Sprache) wird ein Leitfaden für das Planen einer Bereitstellung von DPM, eine Anleitung zum Installieren und Konfigurieren von DPM sowie eine Einführung in die Benutzeroberfläche von DPM bereitgestellt. Das Handbuch steht auf der TechNet-Website zu Data Protection Manager zur Verfügung.
Data Protection Manager 2006 Management Pack-Handbuch	Das DPM 2006 Management Pack-Handbuch beschreibt Überwachungsszenarios, Anweisungen zur Bereitstellung und Aufgaben für den Betrieb von DPM Management Pack für Microsoft Operations Manager 2005 (MOM). Das Handbuch ist auf der Website für die Produktdokumentation von MOM 2005 (http://go.microsoft.com/fwlink/?linkid=43706) (in englischer Sprache) erhältlich.
Häufig gestellte Fragen zu DPM (FAQ)	Mit dem DPM-FAQ wird eine Kurzreferenz für Produktinformationen und eine Anleitung zur Aktualisierung von DPM Beta and DPM Evaluation Edition auf DPM 2006 bereitgestellt. Das FAQ steht auf der TechNet-Website Data Protection Manager (http://go.microsoft.com/fwlink/?linkid=46349) (in englischer Sprache) zur Verfügung.
Technische Referenzartikel	Technische Referenzartikel bieten Informationen über spezifische Themen in Bezug auf DPM. Artikel stehen auf der Produktwebsite von Data Protection Manager (http://go.microsoft.com/fwlink?linkid=33686) zur Verfügung.

Microsoft Knowledge Base-Artikel	Microsoft Knowledge Base-Artikel bieten schnelle, genaue Antworten auf Fragen zu DPM und Lösungen zu häufigen Problemen. Die Artikel stehen auf der Website Microsoft Hilfe und Support (http://go.microsoft.com/fwlink/?linkid=46538) zur Verfügung.

Produktsupportinformationen

Von Microsoft werden eine Reihe von Websites zur Verfügung gestellt, auf denen Sie weitere Informationen über DPM finden können.

- Auf der Website zu Data Protection Manager (http://go.microsoft.com/fwlink?linkid=33686) können Sie sich über DPM informieren und entscheiden, ob DPM als mögliche Lösung für Ihre Probleme beim Schutz von Daten in Frage kommt. Hier können Sie außerdem aktuelle Artikel über neue Entwicklungen zum Schutz von Daten nachlesen.
- Informationen über technischen Support zu DPM finden Sie auf der TechNet-Website Data Protection Manager (http://go.microsoft.com/fwlink/?linkid=43087, in englischer Sprache). Diese Site bietet Informationsressourcen zur Bewertung, Planung, Bereitstellung, Konfiguration, Ausführung und Problembehebung von DPM.
- Auf der Website Microsoft Hilfe und Support (http://go.microsoft.com/fwlink/?LinkId=45276) finden Sie Kontaktinformationen von Microsoft Product Support Services und die Microsoft Knowledge Base mit schnellen, genauen Antworten auf Fragen zu Microsoft-Technologien.

KAPITEL 1

Funktionen von Data Protection Manager: Übersicht

Welche Aufgaben sollten nach dem Installieren, Konfigurieren und Bereitstellen von Microsoft System Center Data Protection Manager 2006 (DPM) durchgeführt werden? Wie kann Effizienz und Zuverlässigkeit gewährleistet werden? Wie werden Probleme beim Hinzufügen von Mitgliedern zu einer Schutzgruppe oder beim Wiederherstellen einer Datei behandelt? In diesem Kapitel wird eine Übersicht über DPM-Vorgänge bereitgestellt, indem einige wichtige Szenarios beschrieben werden, die nach Bereitstellen von DPM auftreten können. Außerdem wird in diesem Kapitel auf DPM-Dokumentationen verwiesen, die für eine fehlerfreie Ausführung von DPM hilfreich sind.

Nehmen Sie für dieses Kapitel einmal an, Sie seien ein Systemadministrator bei Northwind Traders, einem fiktiven Unternehmen, das für die hier beschriebenen Beispiele erdacht wurde, und bei dem Sie nach der Bereitstellung von DPM für Verwaltung und Support zuständig sind.

In diesem Kapitel

DPM-Bereitstellung bei Northwind Traders

Überwachen von DPM-Vorgängen

Verwenden von DPM zum Wiederherstellen von Daten

Überwachen der Leistung von DPM

Warten von DPM-Servern und Dateiservern

Archivieren von DPM für die Notfall-Wiederherstellung

Beheben von Fehlern in DPM-Vorgängen

DPM-Bereitstellung bei Northwind Traders

Northwind Traders ist ein Unternehmen mit 50 Standorten in den USA, die zum Teil über mehrere Dateiserver verfügen. Alle 50 Standorte und deren Dateiserver werden durch drei DPM-Server in einem Rechenzentrum fortlaufend geschützt.

Die DPM-Server sind so konfiguriert, dass auf ihnen Daten gespeichert werden, die bis zu 21 Tage alt sind. Bandsicherungen für langfristige Aufbewahrung und Offsitesicherungen werden von Replikaten auf den DPM-Servern erstellt, sodass Zweigstellen vom Aufwand für die Verwaltung lokaler Bänder befreit sind. DPM stellt automatischen Offsitespeicherschutz zur Verfügung, da sich die DPM-Server in zentralisierten Rechenzentren befinden.

Northwind Traders verwendet Microsoft Operations Framework (MOF), um IT-Vorgänge zu verwalten. MOF ist eine Sammlung optimaler Methoden, Prinzipien und Modelle, durch die IT-Dienstverwaltungsprozesse in jedem Stadium ihrer Lebenszyklen verbessert werden können. In Abbildung 1.1 werden die vier MOF-Quadranten dargestellt, die dem IT-Lebenszyklus entsprechen. Die erste Bereitstellung von DPM bei Northwind Traders war von den Dienstverwaltungsfunktionen im Quadranten „Changing“ (Änderung) abhängig: Änderungsverwaltung, Konfigurationsverwaltung und Veröffentlichungsverwaltung.

Abbildung 1.1 MOF-Quadranten

Hinweis

Microsoft hat DPM in der eigenen Umgebung bereitgestellt. Ausführliche Informationen zur Implementierung von DPM bei Microsoft finden Sie unter „Case Study: Learn How Microsoft Saves US$2.7 Million with DPM“ auf der DPM-Produktwebsite (http://go.microsoft.com/fwlink?linkid=33686, in englischer Sprache).

Wichtige Dokumentationen:

Als Mitglied des Teams, das die DPM-Struktur für Northwind Traders geplant hat, haben Sie die Anleitung im Planungs- und Bereitstellungshandbuch von DPM 2006 (http://go.microsoft.com/fwlink/?LinkId=46351, in englischer Sprache) verwendet.

Für optimale Methoden zur Verbesserung des Bereitstellungsprozesses haben Sie sich über Microsoft Operations Framework (http://go.microsoft.com/fwlink/?LinkId=51208, in englischer Sprache) informiert.

Überwachen von DPM-Vorgängen

Nach Abschluss der DPM-Bereitstellung sind Sie für die Verwaltung des täglichen Betriebs der DPM-Server verantwortlich. In erster Linie möchten Sie natürlich sicherstellen, dass Daten erfolgreich geschützt werden und geschützte Daten wiederhergestellt werden können. Diese Aufgaben gehören zu den Dienstverwaltungsfunktionen, die in den in Abbildung 1.1 dargestellten MOF-Quadranten „Operating“ (Betrieb) und „Supporting“ (Support) auftreten. Die Hauptziele einer Dienstüberwachung und -steuerung sind die Überwachung des Zustands von IT-Diensten und das Ergreifen von Hilfsmaßnahmen zum Minimieren der Auswirkungen von Dienstvorfällen und Systemereignissen.

Obwohl Sie wissen, dass Sie den Status von Aufträgen zum Schutz von Daten überprüfen können, indem Sie für jeden DPM-Server die DPM-Verwaltungskonsole öffnen und im Aufgabenbereich **Überwachung** die Registerkarte **Warnungen** anzeigen können, um nach Warnungen zu suchen, haben Sie sich dazu entschieden, diese empfohlene tägliche Überwachungsaufgabe zu automatisieren. Abonnieren Sie hierzu E-Mail-Benachrichtigungen für wichtige und andere Warnungen. Der DPM-Server erstellt E-Mail-Benachrichtigungen und sendet diese über einen SMTP-Server an die angegebenen Adressen und Verteilerlisten. Für jede Warnung empfangen Sie automatisch eine E-Mail-Benachrichtigung.

Um der IT-Vereinbarung zum Servicelevel (SLA – Service Level Agreement) zu entsprechen, sollten Sie wichtige Warnungen sofort behandeln. Aus diesem Grund richten Sie in Microsoft Outlook Regeln ein, um eingehende Benachrichtigungen zu verwalten. Alle DPM-Benachrichtigungen werden an einen bestimmten Ordner gesendet, und wichtige Benachrichtigungen werden gekennzeichnet. Wenn Sie eine wichtige Warnung empfangen, können Sie die für die Fehlerbehebung erforderlichen Maßnahmen einleiten.

Jede Woche überprüfen Sie die Informationswarnungen, die erstellt wurden, um Trends und mögliche Probleme zu ermitteln. Obwohl Sie bereits bei Problemen mit Schutzgruppen in jedem Fall eine Benachrichtigung erhalten, wird auf der DPM-Verwaltungskonsole im Aufgabenbereich **Schutz von Daten** eine Übersicht des Status aller Schutzgruppen angezeigt.

Die IT-Abteilung von Northwind Traders möchte nächstes Jahr Microsoft Operations Manager 2005 (MOM) in der Domäne bereitstellen. Sie begrüßen die Implementierung von MOM, da sie dann alle DPM-Server mit dem Microsoft System Center Data Protection Manager 2006 (DPM) Management Pack zentral überwachen können.

Wichtige Dokumentationen:

In der DPM-Hilfe (http://go.microsoft.com/fwlink/?linkid=46350, in englischer Sprache) finden Sie eine schrittweise Anleitung für die folgenden Aufgaben:

• Subscribing to notifications (http://go.microsoft.com/fwlink/?LinkId=51903, in englischer Sprache)

• Monitoring alerts (http://go.microsoft.com/fwlink/?LinkId=51904, in englischer Sprache)

• Resolving alerts (http://go.microsoft.com/fwlink/?LinkId=51906, in englischer Sprache)

• Interpreting reports (http://go.microsoft.com/fwlink/?LinkId=51905, in englischer Sprache)

Tipps zum Entwickeln eines Überwachungszeitplans und einen Leitfaden zum Ermitteln von Informationen finden Sie in diesem Handbuch im Kapitel „Überwachen von Data Protection Manager“ (http://go.microsoft.com/fwlink/?LinkId=46365). Dieses Kapitel ist auch hilfreich beim Konfigurieren von Filterregeln in Outlook, um das Verwalten der E-Mail-Benachrichtigungen zu vereinfachen.

Informationen zur Verwendung von DPM Management Pack finden Sie im Microsoft System Center Data Protection Manager 2006 Management Pack-Handbuch (http://go.microsoft.com/fwlink/?linkid=43706, in englischer Sprache).

Verwenden von DPM zum Wiederherstellen von Daten

Sie stellen fest, dass Northwind Traders seine Produktivität steigern und Verwaltungskosten erheblich verringern kann, wenn Sie die Endbenutzerwiederherstellung für unterstützte Clientcomputer aktivieren. Nachdem Ihre Änderungsanforderung geprüft und genehmigt wurde, konfigurieren Sie die Endbenutzerwiederherstellung für die Clientcomputer, auf denen Windows XP ausgeführt wird, in der Domäne. Stellen Sie außerdem sicher, dass die betroffenen Benutzer für die Verwendung dieser Funktion geschult werden.

Benutzer auf diesen Computern können nun Dateien ohne Administrator- oder Helpdeskunterstützung wiederherstellen. Die Dateien werden von den Schattenkopien auf dem DPM-Server abgerufen, die Benutzer erfahren hiervon jedoch nichts.

Andere Benutzer wenden sich direkt an Sie, wenn Dateien wiederhergestellt werden müssen. Die Wiederherstellung ist eine schnelle und einfache Prozedur, die für die Durchführung nur wenige Minuten benötigt. Da Sie jetzt eine sofortige Wiederherstellung bereitstellen können, ohne nach einem Bandarchiv suchen zu müssen oder dieses zu laden, wird die Anzahl erfolgreicher Dateiwiederherstellungen erhöht und der Zeitaufwand für jede einzelne Wiederherstellung verringert.

Wichtige Dokumentationen:

In der DPM-Hilfe (http://go.microsoft.com/fwlink/?linkid=46350, in englischer Sprache) finden Sie eine schrittweise Anleitung für die folgenden Aufgaben:

• Recovering Data (http://go.microsoft.com/fwlink/?LinkId=51984, in englischer Sprache)

• Configuring end-user recovery (http://go.microsoft.com/fwlink/?LinkId=52026, in englischer Sprache).

Wenn bei der Datenwiederherstellung und der Endbenutzerwiederherstellung Probleme auftreten, finden Sie Informationen hierzu in diesem Handbuch im Kapitel „Problembehandlung“ (http://go.microsoft.com/fwlink/?LinkId=46369).

Informationen zum Ermitteln optimaler Methoden zum Ändern der IT-Umgebung finden Sie unter Service Management Functions (http://go.microsoft.com/fwlink/?LinkId=51209, in englischer Sprache).

Überwachen der Leistung von DPM

Obwohl Sie keine Beschwerden über Serververzögerungen erhalten haben, möchten Sie Probleme so früh wie möglich erkennen und optimale Methoden des SMF zur Dienstüberwachung und -steuerung im MOF-Quadranten „Operating“ (Betrieb) anwenden. Konfigurieren Sie hierzu in der **Verwaltung** von Windows unter Verwendung der Option **Leistung** für jeden Dateiserver Leistungswarnungen. Sie können in DPM außerdem regelmäßig den Netzwerkverkehrbericht erstellen, um die Aktivität zwischen DPM-Servern und Dateiservern zu überwachen. Leistungswarnungen dienen dem Verwalten von Ereignissen bei deren Auftreten. Mit Berichten stehen langfristige Daten bereit, um Trends und mögliche Probleme zu erkennen.

Wenn Sie den Netzwerkverkehrbericht überprüfen, stellen Sie fest, dass einer der Dateiserver durchgängig über eine Datenänderungsrate von mehr als 20 % verfügt. Sie führen den Datenträgerauslastungsbericht aus und überprüfen die Datenträgerauslastung für diesen Server. Im Speicherpool ist immer noch ausreichend Speicherplatz zugewiesen, jedoch bemerken Sie, dass die durchschnittliche Auslastung des Synchronisierungsprotokolls 85 % übersteigt. Sie reagieren durch Erhöhen der Datenträgerzuweisung für das Synchronisierungsprotokoll für jeden Server in dieser Schutzgruppe.

Ihr Vorgesetzter teilt Ihnen mit, dass dem Standort Des Moines bald ein neuer Server hinzugefügt wird. Einige Tage später erhalten Sie von DPM eine Warnung, dass ein neuer Server entdeckt wurde. Sie vergleichen die Auslastungen und Kapazitäten der DPM-Server, um den Server zu ermitteln, der zum Schutz des neuen Dateiservers verwendet werden sollte.

Wichtige Dokumentationen:

In der DPM-Hilfe (http://go.microsoft.com/fwlink/?linkid=46350, in englischer Sprache) finden Sie eine schrittweise Anleitung für die folgenden Aufgaben:

- Interpreting reports (http://go.microsoft.com/fwlink/?linkid=51905, in englischer Sprache)
- Modifying disk allocations (http://go.microsoft.com/fwlink/?linkid=51981, in englischer Sprache)
- Configuring protection (http://go.microsoft.com/fwlink/?LinkId=52028, in englischer Sprache)
- Beheben des mit der Warnung „New servers found“ (Neue Server gefunden) verbundenen Fehlers (http://go.microsoft.com/fwlink/?LinkId=52027, in englischer Sprache)

Informationen zum Planen des Schutzes von Daten finden Sie im Planungs- und Bereitstellungshandbuch von DPM 2006 (http://go.microsoft.com/fwlink/?LinkId=46351, in englischer Sprache).

Richtlinien für die Leistungsdatenerfassung und Leistungssteigerung finden Sie in diesem Handbuch im Kapitel „Verwalten der Leistung“ (http://go.microsoft.com/fwlink/?LinkId=46366).

Warten von DPM-Servern und Dateiservern

Als Teil des Serverwartungsplans achten Sie auf die Anwendung von Betriebssystemaktualisierungen für DPM-Server und Dateiserver. Da für einige Aktualisierungen ein Neustart des Servers erforderlich ist, koordinieren Sie die Aktualisierungen mit dem DPM-Schutzzeitplan, sodass der Serverneustart keine Auswirkungen auf geplante Aufträge hat.

Um sicherzustellen, dass Sie gegebenenfalls eine Notfall-Wiederherstellung durchführen können, erstellen und warten Sie ASR-Sätze (Automated System Recovery – automatische Systemwiederherstellung) für jeden DPM- und Dateiserver. Dies ist bei der vollständigen Wiederherstellung eines Servers zum Hinzufügen neuer Hardware von Nutzen. In diesem Fall können Sie den ASR-Satz zum Wiederherstellen des Systemstatus verwenden.

Nachdem DPM für einige Monate ausgeführt wurde, bemerken Sie, dass der für eine der Schutzgruppenreplikate zugewiesene Speicherplatz bald nicht mehr ausreicht. Da sämtlicher Speicherplatz des Speicherpools zugewiesen ist, fügen Sie dem DPM-Server neue Datenträger hinzu und erhöhen die Speicherzuweisung für die Schutzgruppe.

Wichtige Dokumentationen:

Richtlinien zur Serverwartung und Anweisungen zu Änderungen an DPM-Servern und Dateiservern, nachdem der Schutz von Daten konfiguriert wurde, finden Sie in diesem Handbuch im Kapitel „Verwalten von Servern“ (http://go.microsoft.com/fwlink/?LinkId=46367).

Archivieren von DPM für die Notfall-Wiederherstellung

Als Teil der Strategie zur Notfall-Wiederherstellung verwaltet Northwind Traders ein Archiv mit spezifischen Dateien, die das Unternehmen aus rechtlichen Gründen speichern muss. Durch die Notfall-Wiederherstellung wird die SMF zur Speicherverwaltung im MOF-Quadranten „Operating“ (Betrieb) implementiert. Sie verwenden Sicherungssoftware, die DPM unterstützt, um das Übertragen von Daten auf Band zu erleichtern. Da Sie Archive mit DPM-Replikaten erstellen, hat dies keine Auswirkungen auf die Dateiserver. Das heißt, dass Sie während der ordentlichen Geschäftszeit Sicherungen erstellen können.

Darüber hinaus können Sie von den DPM-Datenbanken eine Bandsicherung erstellen und diese wöchentlich aktualisieren. Obwohl kein DPM-Server ausgefallen ist, haben Sie die Sicherungslösung getestet, um zu gewährleisten, dass Sie jeden DPM-Server bei Bedarf wiederherstellen können.

Wichtige Dokumentationen:

In der DPM-Hilfe finden Sie eine schrittweise Anleitung zum Wiederherstellen von Daten (http://go.microsoft.com/fwlink/?LinkId=51984, in englischer Sprache).

Richtlinien zum Wiederherstellen des Schutzes für einen Dateiserver nach einem Datenträgerfehler finden Sie in diesem Handbuch im Kapitel „Verwalten von Servern“ (http://go.microsoft.com/fwlink/?LinkId=46367).

Eine Anleitung zum Sichern von DPM-Replikaten und -Datenbanken sowie zum Wiederherstellen von Daten von einer Bandsicherung auf Dateiservern und DPM-Servern finden Sie in diesem Handbuch im Kapitel „Archivieren und Wiederherstellen von Daten“ (http://go.microsoft.com/fwlink/?LinkId=46368).

Beheben von Fehlern in DPM-Vorgängen

Während der ersten Monate der Verwendung von DPM tritt beim Durchführen mancher Aufgaben gelegentlich ein Fehler auf. Diese Fehler können behoben werden, indem Sie die in der Fehlermeldung empfohlene Maßnahme ergreifen.

Wichtige Dokumentationen:

Eine Anleitung zur Behandlung spezieller und allgemeiner Probleme finden Sie in diesem Handbuch im Kapitel „Problembehandlung“ (http://go.microsoft.com/fwlink/?LinkId=46369).

KAPITEL 2

Überwachen von Data Protection Manager

Nachdem Sie den Schutz von Daten eingerichtet haben, sollten Sie die DPM-Aktivität überwachen, um eine ordnungsgemäße Funktion zu gewährleisten und gegebenenfalls auftretende Probleme zu behandeln. Die Überwachung ist entscheidend, um einen Überblick über vergangene, aktuelle und geplante Vorgänge zu erhalten. Durch eine Überwachung von DPM können Sie sicherstellen, dass alle Aktivitäten zum Schutz von Daten ordnungsgemäß durchgeführt werden, und dass Sie über gegebenenfalls auftretende Fehler und Warnungen benachrichtigt werden.

Dieses Kapitel beginnt mit einem Vorschlag für einen Überwachungszeitplan und einer Referenztabelle, mit der Sie Informationen einholen können, die zur Behandlung von Problemen oder Trends erforderlich sind, die von DPM ermittelt werden. In den weiteren Abschnitten werden Erklärungen und ausführlichere Informationen zu Methoden bereitgestellt, mit denen Sie DPM überwachen können. Des Weiteren wird eingehender erläutert, wie Sie die in der Referenztabelle aufgeführten Ressourcen nutzen können.

In diesem Kapitel

Einrichten eines Überwachungszeitplans

Suchen nach Informationen

Methoden zur Überwachung

- DPM-Verwaltungskonsole
  - Aufgabenbereich **Überwachung**: **Warnungen**
  - Aufgabenbereich **Überwachung**: **Aufträge**
  - Aufgabenbereich **Schutz von Daten**
  - Aufgabenbereich **Verwaltung**: **Datenträger**
  - Aufgabenbereich **Verwaltung**: **Agents**
  - Aufgabenbereich **Berichterstellung**
- Berichte und Warnbenachrichtigungen in E-Mails
- DPM Management Pack

Einrichten eines Überwachungszeitplans

Nachdem Sie mit dem Schutz der Daten begonnen haben, muss in die DPM-Vorgänge nur noch wenig eingegriffen werden. Wenn in einer Situation Maßnahmen ergriffen werden müssen, werden Sie durch eine Warnung darüber informiert. Informationen darüber, wie Sie auf Warnungen reagieren, finden Sie in der Data Protection Manager-Hilfe im Abschnitt „Resolving Alerts“ (http://go.microsoft.com/fwlink/?LinkId=51906, in englischer Sprache). Es wird empfohlen, dass Sie einen Überwachungszeitplan einrichten und diesen regelmäßig befolgen, sodass Sie über Trends und Probleme informiert sind. Des Weiteren unterstützt ein solcher Zeitplan die schnelle Reaktion auf Probleme, die Ihrer Aufmerksamkeit bedürfen. In Tabelle 2.1 werden Vorschläge für einen Überwachungszeitplan aufgeführt.

Tabelle 2.1 Vorschlag für einen Überwachungszeitplan

Zeitraum	Zu überprüfende Quellen	Zu überprüfende Informationen
Täglich	• Wichtige und andere Warnungen • E-Mail-Benachrichtigungen (wenn konfiguriert)	Probleme mit Replikaten und Agents
Wöchentlich	• Informationswarnungen • Status aller geschützten Elemente. Durch Farbe und Form der visuellen Anzeige werden Informationen zu ihrem aktuellen Status bereitgestellt. Siehe Tabelle 2.3.	• Mitgliedschaftsänderungen • Neue Server, die gegebenenfalls geschützt werden müssen • Fehlertrend für Schattenkopien • Visuelle Anzeigen. Wenn alle Anzeigen grün dargestellt werden, sind die Datenquellen erfolgreich geschützt.
Monatlich	Berichte: • Administratorwiederherstellung • Datenträgerauslastung • Netzwerkverkehr • Synchronisierung • Schattenkopien	Trends und Muster, die auf (mögliche) Probleme hindeuten
Bei Bedarf	Status des Wiederherstellungsauftrags	Fehler bei Wiederherstellungsaufträgen

Suchen nach Informationen

Nach Implementieren des Überwachungszeitplans werden Sie bestimmte Trends feststellen und einige Warnungen bemerken. Sie können die Warnungen und damit verbundene Probleme untersuchen, Fehler beheben oder einige der Trends analysieren. DPM stellt einige Ressourcen bereit, die bei der Durchführung dieser Aufgaben hilfreich sind. In Tabelle 2.2 werden einige Referenzen aufgeführt, mit denen Sie nach Informationen suchen können, die bei der Beantwortung häufiger Fragen hilfreich sind.

Tabelle 2.2 Informationsquellen

Fragestellung	Quelle
Liegt ein zu untersuchendes Problem vor? Sind neue Server vorhanden, die zurzeit nicht geschützt sind? Sind auf geschützten Dateiservern Änderungen vorhanden, die sich auf den Schutz von Daten auswirken?	• Ggf. abonnierte E-Mail-Benachrichtigungen mit Warnungen – oder – • Aufgabenbereich **Überwachung**, Registerkarte **Warnungen**

Muss dem Speicherpool Speicherplatz hinzugefügt werden?	• Aufgabenbereich **Überwachung**, Registerkarte **Datenträger** – oder – • Datenträgerauslastungsbericht
Wann werden Aufträge durchgeführt? Wie viel Zeit nahm die letzte Konsistenzprüfung in Anspruch? Welche Datenmenge wurde durch den neuesten Synchronisierungsauftrag übertragen?	• Aufgabenbereich **Überwachung**, Registerkarte **Aufträge**
Wie viele Schattenkopien stehen für ein Volume zur Verfügung? Sind alle Replikate konsistent?	• Aufgabenbereich **Schutz von Daten**, Bereich **Details** – oder – • Aufgabenbereich **Schutz von Daten**: Klicken Sie auf **Schattenkopien verwalten** – oder – • Aufgabenbereich **Wiederherstellung**
Wurde ein Wiederherstellungsauftrag erfolgreich abgeschlossen?	• Aufgabenbereich **Überwachung**, Registerkarte **Warnungen** – oder – • Aufgabenbereich **Überwachung**, Registerkarte **Aufträge** – oder – • E-Mail-Benachrichtigung. (Wenn beim Starten einer Wiederherstellung E-Mail-Benachrichtigungen abonniert werden.)
Kann der DPM-Server mit jedem geschützten Dateiserver eine Verbindung herstellen?	• Aufgabenbereich **Verwaltung**, Registerkarte **Agents**
Welchen Status hat der DPM-Dienst?	• MMC (Microsoft Management Console), Dienste-Snap-In – und – • Ereignisprotokoll bei Dienstfehlern
Welche Probleme sind im letzten Monat aufgetreten?	Aufgabenbereich **Überwachung**, Registerkarte **Warnungen**, **Inaktive Warnungen anzeigen** aktiviert
Welchen Status haben die DPM-Server und die von diesen geschützten Dateiserver?	MOM-Operatorkonsole, Statusansicht

Methoden zur Überwachung

So können Sie Aktivitäten zum Schutz von Daten überwachen

- Mit der DPM-Verwaltungskonsole zeigen Sie DPM-Vorgänge an, die auf einem bestimmten DPM-Server ausgeführt werden.
- Konfigurieren Sie DPM, um Berichte und Benachrichtigungen über Warnungen per E-Mail bereitzustellen. Eine Anleitung hierzu finden Sie in der Data Protection Manager-Hilfe im Abschnitt „How to subscribe to notifications“ (http://go.microsoft.com/fwlink/?LinkId=51903, in englischer Sprache).
- Überwachen Sie Vorgänge für mehrere DPM-Server mithilfe von Microsoft System Center DPM Management Pack für Microsoft Operations Manager 2005 (MOM).

DPM-Verwaltungskonsole

Um die DPM-Verwaltungskonsole zu verwenden, müssen Sie auf einem DPM-Server mit einem Konto angemeldet sein, das auf diesem Server über die Rechte eines Administrators oder Sicherungs-Operators verfügt. An der DPM-Verwaltungskonsole können nicht mehrere Benutzer gleichzeitig angemeldet sein.

In diesem Abschnitt wird jeder Aufgabenbereich der DPM-Verwaltungskonsole erläutert und beschrieben, welche Informationen durch diesen Aufgabenbereich bereitgestellt werden. Wie Sie Tabelle 2.1, „Vorschlag für einen Überwachungszeitplan“, entnehmen können, müssen Sie nicht jeden Aufgabenbereich in der DPM-Verwaltungskonsole überwachen. Eine Übersicht über die DPM-Verwaltungskonsole finden Sie im Planungs- und Bereitstellungshandbuch von DPM im Anhang A: "Verwenden der DPM-Verwaltungskonsole" (http://go.microsoft.com/fwlink/?LinkId=46361).

Folgende Themen werden in diesem Abschnitt behandelt:

- Aufgabenbereich **Überwachung**: **Warnungen**
- Aufgabenbereich **Überwachung**: **Aufträge**
- Aufgabenbereich **Schutz von Daten**
- Aufgabenbereich **Verwaltung**: **Datenträger**
- Aufgabenbereich **Verwaltung**: **Agents**
- Aufgabenbereich **Berichterstellung**

Aufgabenbereich „Überwachung“: „Warnungen“

Auf der Registerkarte **Warnungen** finden Sie folgende Informationen:

- Aktuelle Probleme (wichtige Warnungen)
- Potenzielle Probleme (Warnungen)
- Wichtige Aktivitäten (Informationswarnungen)
- Empfohlene Maßnahmen

Auf der Registerkarte **Warnungen** werden Fehler, Warnungen und Informationsmeldungen angezeigt. Warnungen können nach Schutzgruppe, Server oder Schweregrad gruppiert werden. Sie können außerdem auswählen, ob nur aktive Warnungen oder sowohl aktive als auch inaktive Warnungen angezeigt werden. Inaktive Warnungen sind Warnungen, deren zugrunde liegendes Problem bereits behoben wurde. Darüber hinaus können Sie Benachrichtigungen abonnieren, sodass Sie Warnungen per E-Mail empfangen.

Von DPM wird sichergestellt, dass in der Ansicht **Warnungen** die Probleme wiedergegeben werden, die im System zurzeit aktiv sind. Wenn das Problem behoben wird, durch das eine Warnung erzeugt wurde, wird diese Warnung inaktiv. Tatsächlich müssen für viele Probleme, für die eine Warnung ausgegeben wird, keinerlei Maßnahmen ergriffen werden, da diese Probleme auf eine vorübergehende Situation zurückzuführen sind oder automatisch behoben werden. Beispielsweise kann eine Warnung darauf hindeuten, dass der DPM-Server nicht in der Lage ist, mit einem Dateiserver eine Verbindung herzustellen. In diesem Fall kann die Ursache ein vorübergehendes Netzwerkproblem sein, und ein weiterer Versuch ist unter Umständen erfolgreich. In manchen Fällen wird eine Informationswarnung von DPM nach einer vordefinierten Zeitdauer automatisch als inaktiv festgelegt. Die Warnung „Wiederherstellungssammlung erfolgreich abgeschlossen“ wird beispielsweise zwei Tage nach Abschluss der Wiederherstellung inaktiv, und die Warnung „Neue Server gefunden“ wird nach sieben Tagen inaktiv.

Weitere Informationen finden Sie in der Data Protection Manager-Hilfe im Abschnitt „Resolving Alerts“ (http://go.microsoft.com/fwlink/?LinkId=51906, in englischer Sprache).

Als allgemeine Richtlinie wird folgende Vorgehensweise empfohlen:

- Zeigen Sie aktive Warnungen an, wenn Sie Ihr Augenmerk auf aktive, aktuelle Probleme richten möchten.
- Verwenden Sie inaktive Warnungen als Informationsquelle, um Trends zu ermitteln oder Probleme zu analysieren.

Aufgabenbereich „Überwachung“: „Aufträge“

Auf der Registerkarte **Aufträge** finden Sie die folgenden Informationen:

- Ausführungszeitpunkt von Aufträgen
- Zeitplan für die Ausführung von Aufträgen
- Welche Aufträge eines bestimmten Typs geplant sind
- Welche Aufträge für einen Dateiserver geplant sind
- Welche Aufträge für eine Schutzgruppe geplant sind
- Welche Aufträge nicht erfolgreich abgeschlossen wurden sowie die Ursache dafür
- Ausführungsdauer von Aufträgen
- Die für einen Auftrag übertragene Datenmenge

Auf der Registerkarte **Aufträge** wird der Status von Aufträgen angezeigt. Aufträge können nach Schutzgruppe, Server, Status oder Typ gruppiert werden, und Sie können Aufträge nach Zeitspanne filtern. Ausführliche Informationen zu einzelnen Aufträgen stehen nur auf der Registerkarte **Aufträge** im Detailbereich zur Verfügung. Ausführliche Informationen zu Auftragsfehlern können für die erweiterte Problembehandlung von Nutzen sein.

Sie können auswählen, ob Sie in der Auftragsliste auch regelmäßig geplante Synchronisierungsvorgänge anzeigen möchten. Es ist jedoch nicht erforderlich, Synchronisierungsaufträge regelmäßig zu überwachen, da Probleme gegebenenfalls auf der Registerkarte **Warnungen** angezeigt werden.

Aufgabenbereich „Schutz von Daten“

Auf der Registerkarte **Schutz von Daten** finden Sie folgende Informationen:

• Status von Volumes und Freigaben in den einzelnen Schutzgruppen

• Konfiguration jeder Schutzgruppe, z. B. Wiederherstellungsziele, Datenträgerzuweisung und Schutzzeitplan

Im Aufgabenbereich **Schutz von Daten** wird der Status jedes geschützten Elements bereitgestellt, einschließlich der in Tabelle 2.3 dargestellten visuellen Anzeigen. Wenn alle visuellen Anzeigen grün dargestellt werden, können Sie darauf vertrauen, dass alle Daten erfolgreich geschützt werden.

Tabelle 2.3 Visuelle Anzeigen im Aufgabenbereich „Schutz von Daten“

Visuelle Anzeige	Aktueller Status
Visual Indicator	Die Datenquelle wird zurzeit erfolgreich geschützt.
	Der Schutz von Daten wird gerade initiiert oder beendet.
	Für die Datenquelle oder ihr Replikat ist zurzeit eine aktive Warnung vorhanden.
	Für die Datenquelle oder ihr Replikat ist zurzeit eine aktive wichtige Warnung vorhanden.

Aufgabenbereich „Verwaltung“: „Datenträger“

Auf der Registerkarte **Datenträger** finden Sie folgende Informationen:

• Kapazität von Datenträgern im Speicherpool (belegter und freier Speicherplatz)

• Status von Datenträgern im Speicherpool

• Geschützte Volumes auf den einzelnen Datenträgern

Auf der Registerkarte **Datenträger** wird eine Liste mit Datenträgern im Speicherpool angezeigt. Außerdem können Sie an dieser Stelle Datenträger zum Pool hinzufügen oder entfernen.

Aufgabenbereich „Verwaltung“: „Agents“

Auf der Registerkarte **Agents** finden Sie folgende Informationen:

• Version bereitgestellter Agents

• Status bereitgestellter Agents

• Verfügbarkeit von Agentlizenzen

Auf der Registerkarte **Agents** wird eine Liste von Datei-Agents angezeigt, die auf Dateiservern bereitgestellt werden. Außerdem können Sie an dieser Stelle Agents installieren und deinstallieren sowie Agents und Agentlizenzen aktualisieren.

Aufgabenbereich „Berichterstellung“

Im Aufgabenbereich **Berichterstellung** der DPM-Verwaltungskonsole können Sie die folgenden Aufgaben durchführen:

• Erstellen und Anzeigen von Berichten zu DPM-Vorgängen

• Planen automatischer Berichterstellung

• Verwalten von Reporting Services-Einstellungen

• Abonnieren von E-Mail-Berichten

Die Berichterstellungsfunktionen in DPM basieren auf Microsoft SQL Server™ Reporting Services. SQL Server Reporting Services enthält ein Berichts-Manager-Tool, das nicht mit DPM installiert wird. Da mit dem Berichts-Manager festgelegte Einstellungen Konflikte mit DPM-Einstellungen hervorrufen können, wird empfohlen, das in SQL Server Reporting Services enthaltene Berichts-Manager-Tool nicht zu installieren,

Sie können die DPM-Berichterstellungsfunktion nach der Installation und Konfiguration von DPM jederzeit aktivieren. Um jedoch sicherzustellen, das DPM über ausreichende Informationen zum Erstellen sinnvoller Berichtsdaten verfügt, wird empfohlen, nach Beginn der Aktivitäten zum Schutz von Daten mit dem Anzeigen von Berichten noch wenigstens einen Tag zu warten. Eine Anleitung zum Aktivieren der DPM-Berichterstellung finden Sie in der DPM-Hilfe unter „Using reports“ (http://go.microsoft.com/fwlink/?LinkId=51907, in englischer Sprache).

Hinweis

Wenn ein DPM-Server eine große Anzahl von Dateiservern schützt, sollten Sie den Zeitplan für die Bereitstellung von E-Mail-Berichten zeitlich staffeln. Wenn Ihre Planung eine Bereitstellung aller 5 Berichte zur selben Zeit vorsieht, können die Speichereinschränkungen von SQL Server Reporting Services möglicherweise das Senden einiger Berichte verhindern.

In Tabelle 2.4 werden die verfügbaren Berichte zusammengefasst und deren Verwendung kurz beschrieben.

Tabelle 2.4 DPM-Berichte

Name des Berichts	Zusammenfassung des Inhalts
Administratorwiederherstellung	Mit dem Administratorwiederherstellungsbericht wird eine Statistik für Wiederherstellungen, die von einem Administrator gestartet wurden, bereitgestellt. Die Anzahl der Wiederherstellungen sowie deren durchschnittliche Größe und Dauer werden für eine festgelegte Zeitspanne aufgeführt. Die Daten werden für jeden Dateiserver bzw. jede Schutzgruppe gesammelt, und für alle Dateiserver bzw. Schutzgruppen aggregiert. Mit diesem Bericht können Sie die folgenden Aufgaben durchführen: • Überprüfen der Art und Weise, wie Datenwiederherstellungsanforderungen behandelt und die Leistung im Vergleich mit SLAs bewertet wird •Unterstützen der Berechnung der Investitionsrendite (ROI – Return on Investment) von DPM.

Datenträgerauslastung	Der Datenträgerauslastungsbericht stellt eine Übersicht über die Datenträgerkapazität, -zuweisung und -auslastung im Data Protection Manager-Speicherpool bereit. Die Daten werden für jeden Dateiserver bzw. jede Schutzgruppe gesammelt, und für alle Dateiserver bzw. Schutzgruppen aggregiert. Mit diesem Bericht können Sie die folgenden Aufgaben durchführen: • Ermitteln von Datenträgerauslastungstrends • Darüber entscheiden, ob Datenträgerzuweisungen für Schutzgruppen geändert und dem Speicherpool Datenträger hinzugefügt werden
Netzwerkverkehr	Mit dem Netzwerkverkehrbericht werden Informationen zum Netzwerkverkehr für Synchronisierungsaufgaben bereitgestellt. In diesem Bericht werden die Datenübertragung und die Dauer von Aufträgen grafisch dargestellt und Informationen zum Datendurchsatz verfügbar gemacht. Die Daten werden für jeden Dateiserver bzw. jede Schutzgruppe gesammelt, und für alle Dateiserver bzw. Schutzgruppen aggregiert. Mit diesem Bericht können Sie die folgenden Aufgaben durchführen: • Ermitteln der Auswirkungen von noch andauernden Replikationsprozessen auf das Netzwerk • Optimieren des Schutzzeitplans
Schattenkopie	Der Schattenkopiebericht stellt eine Statistik zu Erfolgs- und Fehlschlagraten und der Gesamtanzahl von Schattenkopien zur Verfügung, sowie Informationen zum Schutzumfang. Die Daten werden für jedes Volume gesammelt und für alle Volumes aggregiert. Verwenden Sie diesen Bericht, um zu bewerten, in welchem Umfang die Ziele zum Schutz von Daten erreicht wurden.
Synchronisierung	Der Synchronisierungsbericht stellt erfolgreiche und fehlgeschlagene Synchronisierungsaufgaben im Zeitablauf dar. Die Fehlerhäufigkeit wird in 6-Stunden-Schritten über eine Zeitspanne von 24 Stunden dargestellt. Die häufigsten Fehlerursachen werden aufgelistet. Die Daten werden für jeden Dateiserver bzw. jede Schutzgruppe gesammelt, und für alle Dateiserver bzw. Schutzgruppen aggregiert. Verwenden Sie diesen Bericht, um den Prozess zum Schutz von Daten auszuwerten.

Informationen zum Interpretieren von Berichtsdaten finden Sie in der DPM-Hilfe unter „Interpreting Reports“ (http://go.microsoft.com/fwlink/?linkid=51905, in englischer Sprache).

Berichte und Warnbenachrichtigungen in E-Mails

Benachrichtigungen erleichtern Routineaufgaben bei der Überwachung. Statt eine Verbindung mit der DPM-Verwaltungskonsole herzustellen, um gegebenenfalls vorhandene wichtige Warnungen anzuzeigen, können Sie die folgenden Informationen per E-Mail abonnieren:

- Einige oder alle DPM-Berichte mit benutzerdefiniertem Format und Zeitplan.
- Individuelle Benachrichtigung für jede Warnung des abonnierten Typs und eine Benachrichtigung, wenn die Warnung aufgehoben wurde.

Wenn Sie Benachrichtigungen aktivieren oder Berichte abonnieren, sollten Sie in Betracht ziehen, in Microsoft Office Outlook eine Regel einzurichten, um Benachrichtigungs- und Berichts-E-Mails in einem oder mehreren Posteingangsordnern zu filtern. Sie können diese E-Mails mithilfe der **Absenderadresse** oder der **Betreffzeile** filtern. Die **Absenderadresse** der E-Mail-Nachrichten, die Benachrichtigungen oder Berichte enthalten, geben Sie beim Konfigurieren des SMTP-Servers als Adresse an.

Hinweis

In der DPM-Hilfe (http://go.microsoft.com/fwlink/?linkid=46350, in englischer Sprache) finden Sie eine Anleitung für die folgenden Aufgaben: Subscribing to notifications (http://go.microsoft.com/fwlink/?LinkId=51903, in englischer Sprache) Subscribing to reports (http://go.microsoft.com/fwlink/?LinkId=51909, in englischer Sprache) Configuring the SMTP server (http://go.microsoft.com/fwlink/?LinkId=51908, in englischer Sprache)

In Tabelle 2.5 wird eine Liste mit Betreffzeilen bereitgestellt, die in den einzelnen Typen von Warnbenachrichtigungen und DPM-Berichten verwendet werden. Sie können mit dem Text in diesen Betreffzeilen Regeln in Outlook einrichten, um Berichte und Warnbenachrichtigungen in bestimmte Ordner zu filtern.

Tabelle 2.5 Betreffzeilen in E-Mail-Benachrichtigungen

E-Mail-Typ	Betreffzeile
Warnbenachrichtigung	• Data Protection Manager: Informationsbenachrichtigung von *angegebenem Server* • Data Protection Manager: Warnungsbenachrichtigung von *angegebenem Server* • Data Protection Manager: Wichtige Benachrichtigung von *angegebenem Server* • Data Protection Manager: Wiederherstellungsbenachrichtigung von *angegebenem Server*
Benachrichtigung über aufgelöste Warnung	• Data Protection Manager: Aufgelöste Informationsbenachrichtigung von *angegebenem Server* • Data Protection Manager: Aufgelöste Warnungsbenachrichtigung von *angegebenem Server* • Data Protection Manager: Aufgelöste wichtige Benachrichtigung von *angegebenem Server*

Bericht	• Administratorwiederherstellungsbericht von *angegebenem Server* • Datenträgerauslastungsbericht von *angegebenem Server* • Netzwerkverkehrbericht von *angegebenem Server* • Schattenkopiebericht von *angegebenem Server* • Synchronisierungsbericht von *angegebenem Server*

DPM Management Pack

Das Microsoft System Center Data Protection Manager 2006 Management Pack für Microsoft Operations Manager 2005 (MOM) ermöglicht es Administratoren, mit einem MOM-Verwaltungsserver den Schutz von Daten, den Status, den Zustand und die Leistung von mehreren Data Protection Manager-(DPM-)Servern und den entsprechenden geschützten Dateiservern zu überwachen.

Mit der MOM-Operatorkonsole kann ein Administrator gleichzeitig die DPM- und die Netzwerkinfrastruktur überwachen und auf diese Weise Probleme beim Schutz von Daten im Zusammenhang mit anderen Faktoren der System- und Netzwerkleistung analysieren. Mit derselben Konsole kann dieser Administrator andere wichtige Anwendungen wie Microsoft SQL Server und Microsoft Exchange Server überwachen.

Vom MOM-Verwaltungsserver aus können Administratoren die folgenden Überwachungsaufgaben für verwaltete DPM-Server und die entsprechenden geschützten Dateiserver durchführen:

- Zentrales Überwachen von Zustand und Status des Schutzes von Daten und wichtige Leistungsindikatoren von mehreren DPM-Servern und den Dateiservern, die von diesen DPM-Servern geschützt werden.
- Anzeigen des Status sämtlicher Rollen auf DPM-Servern und geschützten Dateiservern.
- Überwachen aktionsgebundener DPM-Warnungen in Zusammenhang mit Replikaterstellung, Synchronisierung und Schattenkopien. DPM Management Pack filtert Warnungen heraus, für die keine Aktion erforderlich ist, z. B. ein gerade ausgeführter Synchronisierungsauftrag.
- Überwachen des Status des Arbeitsspeichers, der CPU und von Datenträgerressourcen auf DPM-Servern und Anzeigen von DPM-Datenbankfehlern über MOM-Warnungen.
- Überwachen von Ressourcennutzung und Leistungstrends für DPM-Server.
- Problemdiagnose und -behandlung auf einem remoten DPM-Server.

DPM Management Pack wird nicht mit DPM geliefert. Es steht kostenlos auf der DPM Management Pack-Downloadsite (http://go.microsoft.com/fwlink/?linkid=50208) zum Herunterladen zur Verfügung.

KAPITEL 3

Verwalten der Leistung

Die Architektur von DPM ist für die Optimierung von Datenträgersicherungen entwickelt worden und stellt eine solide Grundlage für stabile Leistung dar. Trotzdem können sich Maßnahmen zur Konfiguration und Überwachung von DPM auch auf dessen Leistung auswirken. In diesem Kapitel wird erläutert, welche Leistung Sie erwarten können, und wie sie die Leistung von DPM optimieren. Netzwerkgeschwindigkeit, Leistungsmerkmale des Dateiservers, die Menge an geschützten Daten und die Häufigkeit der Änderung dieser Daten sind entscheidend für das Ergebnis.

Weitere Informationen zu Überlegungen in Hinblick auf die Leistung beim Einrichten von DPM in Ihrer Organisation finden Sie im Planungs- und Bereitstellungshandbuch von DPM 2006 unter „Planen einer Bereitstellung“ (http://go.microsoft.com/fwlink/?LinkId=46355).

Eine Anleitung zum Behandeln von Leistungsproblemen finden Sie in diesem Handbuch im Kapitel „Problembehandlung“.

In diesem Kapitel

Auswirkungen von DPM-Vorgängen auf die Leistung

- Replikaterstellung
- Nachverfolgen von Änderungen
- Synchronisierung
- Konsistenzprüfung
- DPM-Prozesse

Erfassen von Leistungsdaten

- Leistungsindikatoren
- Netzwerkverkehrbericht

Verbessern der Leistung

- Ermitteln maximaler Arbeitsauslastungen
- Ändern von Arbeitsauslastungen
  - Verwenden der Netzwerk-Bandbreitenbeschränkung
  - Verwenden von Komprimierung über das Netzwerk
  - Staffeln von Startzeiten für die Synchronisierung
  - Planen von Synchronisierungsaufträgen
  - Planen von Konsistenzprüfungen
  - Manuelles Erstellen von Replikaten
- Erhöhen der Kapazität

Verwalten der Leistung von DPM in einem WAN

Auswirkungen von DPM-Vorgängen auf die Leistung

Eines der Themen, mit denen Sie sich als Administrator auseinandersetzen müssen, ist die Auswirkung von DPM auf System- und Netzwerkressourcen. Die primären Datenübertragungsvorgänge sind die folgenden:

- Replikaterstellung: Dieser Vorgang wird für jedes geschützte Volume einmal ausgeführt.
- Änderungsnachverfolgung: Hierbei handelt es sich um einen fortlaufenden Prozess auf jedem geschützten Dateiserver.
- Synchronisierung: Dieser Vorgang wird auf Grundlage eines regelmäßigen, benutzerdefinierten Zeitplan ausgeführt.
- Konsistenzprüfung: Dieser Vorgang wird im Fall eines inkonsistenten Replikats ausgeführt.

Ein Verständnis dieser Vorgänge und DPM-Prozesse erweist sich beim Ermitteln realistischer Erwartungen für die Leistung als nützlich.

Replikaterstellung

In DPM handelt es sich bei einem Replikat um eine vollständige Kopie der geschützten Daten auf einem einzelnen Volume. Der DPM-Datei-Agent auf dem Dateiserver sendet die zu schützenden Daten an den DPM-Server. Von jedem Volume in der Schutzgruppe wird ein Replikat erstellt. Die Replikaterstellung ist einer der DPM-Vorgänge, für die die meisten Ressourcen erforderlich sind, und benötigt in besonderem Maße Netzwerkressourcen.

Typischerweise wird die Leistung der Replikaterstellung durch die Geschwindigkeit der Netzwerkverbindung zwischen DPM-Server und den Dateiservern begrenzt. Mit anderen Worten, der Zeitaufwand für die Übertragung einer Datenmenge von 1 GB von einem Dateiserver an den DPM-Server wird durch die Datenmenge festgelegt, die im Netzwerk pro Sekunde übertragen werden kann.

In Tabelle 3.1 wird der Zeitaufwand für die Übertragung verschiedener Datenmengen bei unterschiedlichen Netzwerkgeschwindigkeiten unter optimalen Bedingungen dargestellt. Die Zeitangaben sind in Stunden gegeben.

Tabelle 3.1 Zeitaufwand für die Übertragung von Daten über ein Netzwerk bei verschiedenen Geschwindigkeiten

Datengröße	100 Mbit/s	32 Mbit/s	8 Mbit/s	2 Mbit/s	512 Kbit/s
1 GB	< 1 Stunde	< 1	< 1	1,5	6
50 GB	1,5	5	18	71	284
200 GB	6	18	71	284	1.137
500 GB	15	45	178	711	2.844

Mbit/s = Megabit pro Sekunde Kbit/s = Kilobit pro Sekunde

Technische Referenz:

Die Dauer für die Fertigstellung der ersten Replikaterstellung (ER) kann typischerweise wie folgt berechnet werden:

ER: Stunden = ((Datengröße in MB) / (0,8 x Netzwerkgeschwindigkeit in MB/s)) / 3600

Hinweis 1: Die Netzwerkgeschwindigkeit wird von Bit in Byte durch Division mit 8 umgerechnet.

Hinweis 2: Die Netzwerkgeschwindigkeit wird mit 0,8 multipliziert, da die maximale Netzwerkeffizienz ungefähr 80 % beträgt.

In einem äußerst schnellen Netzwerk, z. B. einer Gigabitverbindung, wird die Geschwindigkeit der Replikaterstellung durch die Datenträgergeschwindigkeit des DPM-Servers oder des Dateiservers festgelegt – je nachdem, welche geringer ist.

Die Auswirkungen der Replikaterstellung auf die Netzwerkleistung können durch Verwenden der Netzwerk-Bandbreitenbeschränkung verringert werden. Weitere Informationen finden Sie im Abschnitt „Verwenden der Netzwerk-Bandbreitenbeschränkung“ in diesem Kapitel.

Um die Netzwerkauslastung durch Replikaterstellung zu vermeiden, können Sie Replikate manuell auf Band oder anderen Wechselmedien erstellen. Weitere Informationen finden Sie im Abschnitt „Manuelles Erstellen von Replikaten“ in diesem Kapitel.

Nachverfolgen von Änderungen

Nach Erstellen des Replikats startet der Datei-Agent auf dem Dateiserver die Nachverfolgung von geschützten Daten auf diesem Server. Diese Änderungen werden auf dem Dateiserver in ein Synchronisierungsprotokoll geschrieben. Änderungen an Dateien werden gefiltert, bevor sie auf das Volume geschrieben werden. Dieser Prozess ähnelt dem Filtern von Dateien durch ein Antivirusprogramm und erfordert einen ähnlichen Leistungsaufwand.

Synchronisierung

Synchronisierung ist in DPM die Übertragung von Datenänderungen vom Synchronisierungsprotokoll auf jedem geschützten Volume eines Dateiservers an das Übertragungsprotokoll auf einem DPM-Server und die Anwendung der Änderungen auf ein Replikat der geschützten Daten. Durch Synchronisierung wird gewährleistet, dass die Replikate mit den geschützten Daten auf dem Dateiserver aktualisiert werden. Jeder Synchronisierungsauftrag verwendet Netzwerkressourcen und kann aus diesem Grund die Netzwerkleistung beeinträchtigen.

Die Auswirkungen der Synchronisierung auf die Netzwerkleistung können durch Verwenden der Netzwerk-Bandbreitenbeschränkung und Komprimierung verringert werden. Weitere Informationen finden Sie in den Abschnitten „Verwenden der Netzwerk-Bandbreitenbeschränkung“ und „Verwenden der Komprimierung über das Netzwerk“ in diesem Kapitel.

Konsistenzprüfung

Eine Konsistenzprüfung ist die Suche nach Inkonsistenzen zwischen einem geschützten Volume und seinem Replikat sowie die Korrektur dieser Inkonsistenzen.

Die Leistung des Dateiservers, des DPM-Servers und des Netzwerks wird durch die Ausführung einer Konsistenzprüfung beeinträchtigt. Es wird empfohlen, Konsistenzprüfungen außerhalb der Hauptgeschäftszeiten durchzuführen.

DPM führt in den folgenden Fällen automatisch eine Konsistenzprüfung durch:

- Beim Erstellen eines Replikats für eine neue Schutzgruppe
- Beim Schützen neuer Datenquellen, indem diese einer vorhandenen Schutzgruppe hinzugefügt werden
- Beim Ändern des Speicherplatzes, der dem Synchronisierungsprotokoll zugewiesen wird
- Wenn eine täglich geplante Konsistenzprüfung für eine Schutzgruppe darauf hindeutet, dass das Replikat inkonsistent ist

Wenn die Inkonsistenz eines Replikats auf einen Überlauf des Synchronisierungsprotokolls oder ein unerwartetes Herunterfahren des Dateiservers zurückzuführen ist, muss eine Synchronisierung mit Konsistenzprüfung durchgeführt werden. Sie können manuell auf Konsistenz prüfen oder im Falle einer täglich geplanten Konsistenzprüfung warten, bis von DPM eine Konsistenzprüfung vorgenommen wird.

In der DPM-Hilfe (http://go.microsoft.com/fwlink/?linkid=46350, in englischer Sprache) finden Sie eine Anleitung zum Ausführen von Konsistenzprüfungen.

- Eine Anleitung zum manuellen Durchführen einer Konsistenzprüfung finden Sie unter „How to synchronize a replica“ (http://go.microsoft.com/fwlink/?LinkId=51910, in englischer Sprache).
- Eine Anleitung zum Planen von Konsistenzprüfungen finden Sie unter „How to modify protection options“ (http://go.microsoft.com/fwlink/?LinkId=51911, in englischer Sprache).

DPM-Prozesse

Auf dem DPM-Server sind drei Prozesse von besonderer Bedeutung:

- **DPM-Datei-Agent (MsDpmFsAgent.exe)**. DPM-Aufträge wirken sich sowohl auf die Speicher- als auch auf die CPU-Auslastung durch den DPM-Datei-Agent aus. Es ist nicht ungewöhnlich, dass die CPU-Auslastung durch MsDpmFsAgent.exe während Konsistenzprüfungen ansteigt.
- **DPM-Dienst (MsDpm.exe)**. Der DPM-Dienst wirkt sich sowohl auf die Speicher- als auch die CPU-Auslastung aus.
- **DPM-Verwaltungskonsole (eine Instanz von Mmc.exe)**. Die DPM-Verwaltungskonsole kann für eine hohe Speicherauslastung ausschlaggebend sein. Sie können diese schließen, wenn sie gerade nicht verwendet wird.

Hinweis

Es ist damit zu rechnen, dass die Speicherauslastung für die DPM-Instanz des SQL Server-Dienstes (MicrosoftDPMAcct.exe) vergleichsweise hoch ist. Dies stellt kein Problem dar. Der Dienst verwendet normalerweise eine große Menge an Arbeitsspeicher zum Zwischenspeichern, gibt jedoch bei wenig freiem Arbeitsspeicher diesen wieder frei.

DPM ist mit den meisten verbreiteten Antivirusprogrammen kompatibel. Antivirusprogramme können jedoch die DPM-Leistung beeinträchtigen, wenn einige DPM-Prozesse in Echtzeit überwacht werden. Weitere Informationen finden Sie in diesem Handbuch im Kapitel „Verwalten von Servern“ im Abschnitt „Ausführen von Antivirusprogrammen”.

Erfassen von Leistungsdaten

Für das Erfassen von DPM-Leistungsdaten stehen zwei Methoden zur Verfügung:

• Die in Windows Server 2003 integrierten Leistungsindikatoren

• Der Netzwerkverkehrbericht in DPM

Leistungsindikatoren

Eine Methode zum Überwachen der Leistung von DPM-Servern bietet die Option **Leistung** unter **Verwaltung**. Sie können die überwachten Daten konfigurieren, sodass diese als Protokoll gespeichert werden. Sie können **Leistung** außerdem so konfigurieren, dass Warnungen generiert werden. Informationen zum Erstellen und Konfigurieren von Leistungswarnungen finden Sie im Microsoft Knowledge Base-Artikel 324752, „How to create and configure performance monitor alerts in Windows Server 2003“ (http://go.microsoft.com/fwlink/?LinkId=47881, in englischer Sprache).

Hinweis

Sie können mit dem DPM Management Pack für Microsoft Operations Manager 2005 (MOM) von einem MOM-Verwaltungsserver aus Status, Zustand und Leistung von mehreren DPM-Servern zentral überwachen. Informationen zum Herunterladen des DPM Management Packs finden Sie auf der DPM Management Pack-Downloadseite (http://go.microsoft.com/fwlink/?linkid=50208, in englischer Sprache).

In Tabelle 3.2 werden Indikatoren aufgeführt, die beim Überwachen der Leistung des DPM-Servers von Nutzen sind. Weitere Informationen zu bestimmten Leistungsindikatoren finden Sie in der Hilfe zu Leistungsprotokollen und Warnungen. Klicken Sie auf **Start**, zeigen Sie auf **Verwaltung**, und wählen Sie **Leistung** aus. Klicken Sie im Menü **Aktion** auf **Hilfe**.

Tabelle 3.2 Leistungsindikatoren zur Überwachung von DPM

Leistungsobjekt und -indikator	Beschreibung	Auf ein mögliches Problem hindeutender Wert	Mögliche Ursachen
Arbeitsspeicher: Verfügbare MB	Gibt den freien Arbeitsspeicher für Prozesse an, die auf dem angegebenen DPM-Server ausgeführt werden. Der Wert **Verfügbare MB** stellt den gesamten Arbeitsspeicher dar, der für ausgelagerte Nulllisten, Standbylisten (zwischengespeicherte Listen) und freie Listen reserviert ist.	< 50 MB Weist auf wenig freien Arbeitsspeicher auf dem DPM-Server hin.	• Eine oder mehrere Anwendungen verwenden große Mengen an Arbeitsspeicher. • Mehrere DPM-Aufträge werden gleichzeitig ausgeführt. • Der DPM-Server verfügt nicht über genügend Arbeitsspeicher für die aktuelle DPM-Arbeitsauslastung.

Prozessor: Prozessorzeit (%)	Gibt den prozentualen Anteil der Zeit an, die der Prozessor während des Samplingintervalls ausgelastet ist.	> 95 % für länger als 10 Minuten. Weist auf eine sehr hohe CPU-Auslastung auf dem DPM-Server hin.	• Mehrere DPM-Aufträge werden gleichzeitig ausgeführt. Aufträge zur Synchronisierung mit Konsistenzprüfung führen zu einer besonders hohen CPU-Auslastung. • Auf dem Server ist die Komprimierung über das Netzwerk aktiviert. Die Kompimierung ermöglicht einen höheren Datendurchsatz bei der Replikaterstellung und Synchronisierung, ohne die Netzwerkleistung zu beeinträchtigen. Für dieses Verfahren müssen jedoch sowohl auf dem Dateiserver als auch auf dem DPM-Server große Datenmengen verarbeitet werden. • Ein außer Kontrolle geratener Prozess erschöpft Systemressourcen. • Der DPM-Server verfügt nicht über genügend Verarbeitungska-pazität für die aktuelle DPM-Arbeitsauslastung.

Physikalischer Datenträger: Aktuelle Warteschlangenlänge (für alle Instanzen)	Gibt die Anzahl von Datenträgeranforderungen an, die aktuell ausstehen, und Anforderungen, die zurzeit verarbeitet werden.	> 80 Anforderungen für mehr als 6 Minuten. Weist auf eine zu hohe Warteschlangenlänge von Datenträgern hin.	• Mehrere gleichzeitig ausgeführte DPM-Aufträge fordern große Mengen an Datenträgerres-sourcen an. • Die Datenträgerleistung muss optimiert werden. • Die Datenträgerres-sourcen auf dem DPM-Server sind für die aktuelle DPM-Arbeitsauslastung nicht ausreichend.

Netzwerkverkehrbericht

Auf der ersten Seite des Netzwerkverkehrberichts, der Seite **Zusammenfassung**, wird, wie in den Berichtsparametern angegeben, für alle Dateiserver oder Schutzgruppen auf einem Dateiserver oder einer Schutzgruppenebene eine Netzwerkverkehrstatistik angezeigt. In Abbildung 3.1 werden die in der Netzwerkverkehrzusammenfassung enthaltenen Informationen angezeigt.

Abbildung 3.1 Kopfzeile der Zusammenfassung des Netzwerkverkehrberichts

Synchronization Traffic Summary for all File Servers						
	Duration		Transferred		Throughput	
Total Jobs	Total (in Hours)	Average (in Minutes)	Total (in GB)	Average (in MB)	Average (MB/Minute)	File Server with most data changes

Der Bericht enthält außerdem die durchschnittliche wöchentliche Datenänderungsrate für die ersten 10 Dateiserver oder Schutzgruppen. Die wöchentliche Datenänderungsrate ist das prozentuale Verhältnis der Größe von übertragenen Synchronisierungsdaten zur Größe der geschützten Daten (oder des Volumes).

Auf Grundlage von Stichproben kann eine durchschnittliche tägliche Änderungsrate von mehr als 10 % als hoch angesehen werden und zu Synchronisierungsfehlern führen. Wenn die Datenänderungsrate hoch ist, stellen Sie sicher, dass auf dem Dateiserver im Synchronisierungsprotokoll genügend Speicherplatz vorhanden ist, um Datenänderungen nachzuverfolgen. Darüber hinaus können Sie als Vorsichtsmaßnahme die fast ununterbrochene Synchronisierung aktivieren, wenn diese nicht bereits aktiviert ist. Weitere Informationen finden Sie in der DPM-Hilfe unter „How to modify disk allocation“ und „How to modify protection options“ (http://go.microsoft.com/fwlink/?LinkId=51911, in englischer Sprache).

Verbessern der Leistung

Leistung wird durch Arbeitsauslastung und Kapazität bestimmt. Ein langsamer Computer kann eine ausreichende Leistung erbringen, wenn dieser über eine geringe Arbeitsauslastung verfügt. Im Gegensatz dazu kann die tatsächliche Leistung eines äußerst leistungsstarken Computers beeinträchtigt sein, wenn dieser mit einer übermäßigen Arbeitsauslastung konfrontiert wird. Bei Vorgängen zwischen zwei Computern in einem Netzwerk wird die Arbeitsauslastung, die effektiv bewältigt werden kann, durch die Komponente mit der niedrigsten Kapazität begrenzt. Bei dieser Komponente kann es sich um einen der Computer oder um die Netzwerkverbindung selbst handeln.

Im Allgemeinen können Sie die Leistung steigern, indem Sie Änderungen an Arbeitsauslastung, Kapazität oder beidem vornehmen.

- Weitere Informationen zur Planung der DPM-Konfiguration für optimale Leistung finden Sie im Planungs- und Bereitstellungshandbuch von DPM 2006 (http://go.microsoft.com/fwlink/?LinkId=46351, in englischer Sprache) in den Kapiteln „Planen einer Bereitstellung“ und „Planen einer Strategie zum Schutz von Daten“.
- Informationen zur nicht DPM-spezifischen Leistungsoptimierung finden Sie unter Performance Tuning Guidelines for Windows Server 2003 (http://go.microsoft.com/fwlink/?LinkId=51913, in englischer Sprache).

Ermitteln maximaler Arbeitsauslastungen

In Tabelle 3.3 wird die von einem DPM-Server unterstützte Auslastung für den Schutz von Daten für verschiedene Konfigurationen dargestellt.

In Tabelle 3.3 steht die „Gesamtumfang geschützter Daten" für die Aggregatgröße geschützter Daten auf sämtlichen Dateiservern. Die „Gesamtanzahl geschützter Dateien“ steht für die Aggregatanzahl geschützter Dateien auf sämtlichen Dateiservern. Die „Datenträgergruppe“ wird entweder als einzelner Datenträger oder als RAID-Satz für den angegebenen Speicherpool definiert. In beiden Fällen sollte der Schreibcache aktiviert sein.

Die Empfehlung in jeder Zeile der Tabelle gilt nur, wenn die Daten alle angegebenen Bedingungen erfüllen. Wenn die geschützten Daten eine oder mehrere der angegebenen Bedingungen in einer Zeile der Tabelle überschreiten, überprüfen Sie die Empfehlungen in der folgenden Zeile.

Die verfügbare Netzwerkbandbreite bezieht sich auf die Netzwerkbandbreite, die der DPM-Anwendung für mindestens 8 Stunden am Tag zur Verfügung steht. Wenn das Netzwerk über einen längeren Zeitraum zur Verfügung steht, ist die erforderliche Bandbreite geringer. Wenn weitere Anwendungen das Netzwerk verwenden, ist die gesamte Netzwerkbandbreite, die DPM zur Verfügung steht, geringer.

Tabelle 3.3 Hardwarekonfigurationen und empfohlene maximale Arbeitsauslastungen

Hardwarekonfiguration	Empfohlene maximale Arbeitsauslastung
Prozessor: 500 MHz Arbeitsspeicher: 512 MB Anzahl der Datenträgergruppen: 1 Verfügbare Netzwerkbandbreite: 4 Mbit/s	Gesamtumfang geschützter Daten ≤ 100 GB Gesamtanzahl geschützter Dateien ≤ 500.000 Gesamte tägliche Änderungen ≤ 10 GB

Prozessor: 1 GHz Arbeitsspeicher: 512 MB Anzahl der Datenträgergruppen: 1 Verfügbare Netzwerkbandbreite: 10 Mbit/s	Gesamtumfang geschützter Daten ≤ 250 GB Gesamtanzahl geschützter Dateien ≤ 1.000.000 Gesamte tägliche Änderungen ≤ 25 GB
Prozessor: 2 GHz Arbeitsspeicher: 512 MB Anzahl der Datenträgergruppen: 1 Verfügbare Netzwerkbandbreite: 20 Mbit/s	Gesamtumfang geschützter Daten ≤ 500 GB Gesamtanzahl geschützter Dateien ≤ 10.000.000 Gesamte tägliche Änderungen ≤ 50 GB
Prozessor: 3 GHz Arbeitsspeicher: 512 MB Anzahl der Datenträgergruppen: 1 Verfügbare Netzwerkbandbreite: 72 Mbit/s	Gesamtumfang geschützter Daten ≤ 900 GB Gesamtanzahl geschützter Dateien ≤ 10.000.000 Gesamte tägliche Änderungen ≤ 200 GB
Prozessor: 3 GHz Arbeitsspeicher: 1 GB Anzahl der Datenträgergruppen: 2 Verfügbare Netzwerkbandbreite: 100 Mbit/s	Gesamtumfang geschützter Daten ≤ 1,8 TB Gesamtanzahl geschützter Dateien ≤ 15.000.000 Gesamte tägliche Änderungen ≤ 250 GB
Prozessor: 2 x 3 GHz Arbeitsspeicher: 2 GB Anzahl der Datenträgergruppen: 4 Verfügbare Netzwerkbandbreite: 180 Mbit/s	Gesamtumfang geschützter Daten ≤ 3,6 TB Gesamtanzahl geschützter Dateien ≤ 30.000.000 Gesamte tägliche Änderungen ≤ 500 GB
Prozessor: 2 x 3 GHz Arbeitsspeicher: 3 GB Anzahl der Datenträgergruppen: 8 Verfügbare Netzwerkbandbreite: 250 Mbit/s	Gesamtumfang geschützter Daten ≤ 6 TB Gesamtanzahl geschützter Dateien ≤ 100.000.000 Gesamte tägliche Änderungen ≤ 750 GB

Technische Referenz:

Die erforderliche verfügbare Netzwerkbandbreite kann wie folgt berechnet werden:

Netzwerkgeschwindigkeit in Mbit/s = (tägliche Änderungen in MB) x 8 / (8 Stunden x 3600 x 0,8)

Hinweis 1: Für die Formel wird vorausgesetzt, dass das Netzwerk von DPM 8 Stunden am Tag genutzt werden kann.

Hinweis 2: Die Netzwerkgeschwindigkeit wird mit 0,8 multipliziert, da die maximale Netzwerkeffizienz ungefähr 80 % beträgt.

Ändern von Arbeitsauslastungen

DPM bietet einige Methoden, mit denen Auslastungen beim Schutz von Daten geändert und die Leistung auf diese Weise gesteigert werden kann. In Tabelle 3.4 werden die Methoden aufgeführt, mit denen die entsprechenden Auslastungen geändert werden können, sowie deren zu erwartende Auswirkungen.

Tabelle 3.4 Methoden zum Ändern von Auslastungen beim Schutz von Daten

Methode	Auswirkung
Verwenden der Netzwerk-Bandbreitenbeschränkung	Aufträge verwenden weniger Bandbreite, benötigen jedoch mehr Zeit
Verwenden der Komprimierung über das Netzwerk	Verringert die Größe der Datenübertragung, erhöht jedoch die CPU-Nutzung auf dem DPM-Server und den geschützten Dateiservern
Staffeln von Startzeiten für die Synchronisierung	Gleicht die Auslastung von Synchronisierungsaufträgen zwischen Schutzgruppen aus
Planen von Konsistenzprüfungen außerhalb der Hauptgeschäftszeit	Verhindert, dass die reguläre geschäftliche Verwendung von geschützten Dateiservern durch DPM beeinträchtigt wird
Manuelles Erstellen von Replikaten	Beschleunigt unter Umständen die Replikaterstellung und erfordert keine Netzwerkressourcen oder Leistungsaufwand auf Dateiservern

Verwenden der Netzwerk-Bandbreitenbeschränkung

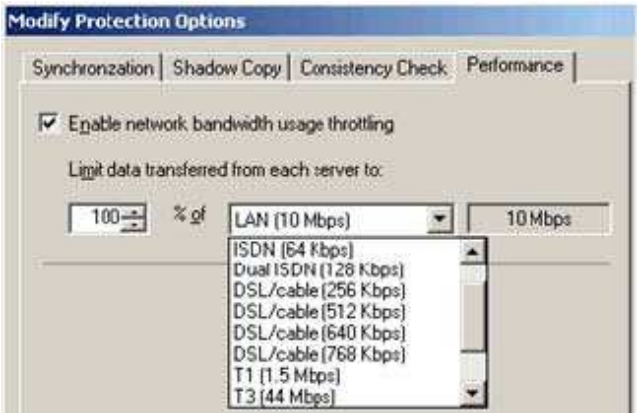
Mithilfe der Netzwerk-Bandbreitenbeschränkung wird die von DPM zum Erstellen und Synchronisieren von Replikaten verwendete Netzwerkbandbreite begrenzt. Die Netzwerk-Bandbreitenbeschränkung dient dazu, anderen Anwendungen als DPM Netzwerkbandbreite zur Verfügung zu stellen.

Der Vorteil einer Verwendung der Netzwerk-Bandbreitenbeschränkung besteht darin, dass die von einem Synchronisierungsauftrag maximal verwendeten Netzwerkressourcen eingeschränkt werden können. Der Nachteil der Netzwerk-Bandbreitenbeschränkung besteht darin, dass der Zeitaufwand für die Fertigstellung von Synchronisierungsaufträgen erhöht werden kann.

Die Netzwerk-Bandbreitenbeschränkung wird für jede Schutzgruppe konfiguriert. Sie wird über einen absoluten Höchstwert von pro Sekunde zu übertragenden Daten angegeben. Wenn Sie beispielsweise einen Höchstwert von 50 % bei einer Verbindungsgeschwindigkeit von 512 Kbit/s angeben, ist die Rate, mit der die Dateiserver in dieser Schutzgruppe Daten versenden, auf 256 Kbit/s beschränkt.

In Abbildung 3.2 wird das Dialogfeld dargestellt, mit dem Sie die Netzwerk-Bandbreitenbeschränkung aktivieren.

Abbildung 3.2 Dialogfeld „Schutzoptionen ändern“



Obwohl Sie die Netzwerk-Bandbreitenbeschränkung über einen prozentualen Anteil der Verbindungsgeschwindigkeit konfigurieren, ist der angewendete Höchstwert der absolute Wert dieser Angabe zum Konfigurationszeitpunkt. Die Bandbreitenbeschränkung wird nicht dynamisch der aktuellen Verbindungsgeschwindigkeit angepasst. Wenn Sie beispielsweise 50 % von einer Verbindungsgeschwindigkeit von 512 Kbit/s angeben, beträgt die Netzwerk-Bandbreitenbeschränkung 256 Kbit/s. Wenn die Verbindung zu einem späteren Zeitpunkt auf eine Geschwindigkeit von 100 Mbit/s aktualisiert wird, beträgt die Netzwerk-Bandbreitenbeschränkung weiterhin 256 Kbit/s.

Beachten Sie beim Auswählen der Netzwerkverbindungsgeschwindigkeit die folgenden Richtlinien:

- **Wenn die tatsächliche Geschwindigkeit des Netzwerks nicht im Menü aufgelistet ist**, wählen Sie die Verbindungsgeschwindigkeit aus, die der tatsächlichen Geschwindigkeit am nächsten kommt.
- **Wenn die tatsächliche Netzwerkgeschwindigkeit zwei Verbindungsgeschwindigkeiten im Menü am nächsten kommt**, wählen Sie die niedrigere Geschwindigkeit aus.

Die Netzwerkbandbreite kann auch durch Gruppenrichtlinien eingeschränkt werden. Die Einschränkung reservierbarer Bandbreite durch Gruppenrichtlinien auf dem lokalen Computer legt die gemeinsame reservierbare Bandbreite aller Programme fest, die den Paketplaner verwenden, DPM eingeschlossen. Durch die DPM-Netzwerk-Bandbreitenbeschränkung wird die Netzwerkbandbreite festgelegt, die von DPM während der Replikaterstellung, Synchronisierung und Konsistenzprüfungen verwendet werden kann. Wenn die DPM-Bandbreitenbeschränkung allein oder zusammen mit Einschränkungen durch andere Programme die Einschränkung reservierbarer Bandbreite durch Gruppenrichtlinien überschreitet, wird die DPM-Bandbreitenbeschränkung unter Umständen nicht angewendet.

Wenn beispielsweise ein DPM-Computer mit einer Netzwerkverbindungsgeschwindigkeit von 1 Gbit/s durch Gruppenrichtlinien über eine Einschränkung reservierbarer Bandbreite von 20 % verfügt, werden von der Bandbreite für alle Programme, die den Paketplaner verwenden, 200 Mbit/s reserviert. Wenn in diesem Fall die DPM-Bandbreitennutzung auf maximal 150 Mbit/s und die Bandbreitennutzung durch Internetinformationsdienste (IIS – Internet Information Services) auf maximal 100 Mbit/s festgelegt wird, übersteigt die Summe der Bandbreitenbeschränkungen von DPM und IIS die durch die Gruppenrichtlinie vorgegebene Einschränkung reservierbarer Bandbreite, und der DPM-Höchstwert findet möglicherweise keine Anwendung.

Um dieses Problem zu beheben, verringern Sie in DPM die Einstellung für die maximale Netzwerk-Bandbreitennutzung. Weitere Informationen finden Sie in der DPM-Hilfe unter „How to synchronize a replica“ (http://go.microsoft.com/fwlink/?linkid=51910, in englischer Sprache).

Verwenden von Komprimierung über das Netzwerk

Durch Komprimierung wird die Größe übertragener Daten während der Replikaterstellung und Synchronisierung verringert und ein größerer Datendurchsatz bei geringeren Auswirkungen auf die Netzwerkleistung ermöglicht. Durch diese Option wird jedoch die CPU-Auslastung sowohl auf dem DPM-Server als auch auf den geschützten Dateiservern erhöht. Der Umfang der Komprimierung und die Steigerung der Netzwerkleistung hängt von der Arbeitsauslastung ab.

Die Komprimierung wird auf Schutzgruppenebene aktiviert und bei der Replikaterstellung, der Synchronisierung und bei Konsistenzprüfungen angewendet. Für Wiederherstellungsaufträge wird die Komprimierung immer verwendet.

Eine Anleitung zum Aktivieren der Komprimierung finden Sie in der DPM-Hilfe unter „How to modify protection options“ (http://go.microsoft.com/fwlink/?linkid=51911, in englischer Sprache).

Staffeln von Startzeiten für die Synchronisierung

Sie können für Synchronisierungsaufträge einzelner Schutzgruppen eine Startzeit in Minuten nach der vollen Stunde angeben. Wenn Sie die Startzeiten staffeln, werden die Auswirkungen auf die Netzwerkleistung durch die Ausführung mehrerer großer Aufträge zum Schutz von Daten minimiert. Synchronisierungsaufträge für verschiedene Dateiserver in derselben Schutzgruppe werden von DPM automatisch in Abständen von 10 Minuten gestaffelt.

- Um zu ermitteln, ob Sie die Startzeiten von Synchronisierungsaufträgen staffeln sollten, sammeln Sie in der DPM-Verwaltungskonsole zunächst Informationen zu geplanten Datenschutzaufträgen:
    - Überprüfen Sie im Netzwerkverkehrbericht die Informationen zu Zeiten hoher Nutzung und erwägen Sie eine Staffelung einiger der Aufträge, die während dieser Zeiten ausgeführt werden.
    - Überprüfen Sie Aufträge im Aufgabenbereich **Überwachung** auf der Registerkarte **Aufträge**, die für Zeiten geplant sind, in denen auf dem DPM-Server lange Warteschlangen von Datenträgern vorhanden sind.
    - Überprüfen Sie im Aufgabenbereich **Schutz von Daten** Schutzgruppendetails, um die Größe und Häufigkeit von Schutzaufträgen zu ermitteln.
- Um die Arbeitsauslastung in DPM zu staffeln, planen Sie die Synchronisierung für einige Schutzgruppen neu:
    - Wenn eine Schutzgruppe über einen fast ununterbrochenen (stündlichen) Synchronisierungszeitplan verfügt, versetzen Sie die Synchronisierungen, sodass diese nicht mehr zur vollen Stunde ausgeführt werden.
    - Wenn Synchronisierungsaufträge geplant sind, sodass diese vor der Erstellung einzelner Schattenkopien für eine Schutzgruppe ausgeführt werden, sollten Sie eine Änderung des Zeitplans für Schattenkopien in Erwägung ziehen.

        Weitere Informationen finden Sie in der DPM-Hilfe unter „How to synchronize a replica“ (http://go.microsoft.com/fwlink/?linkid=51910, in englischer Sprache).

Planen von Synchronisierungsaufträgen

Sie können zwischen zwei Synchronisierungsmodi auswählen: **Nur vor dem Erstellen der Schattenkopie** oder **Fast ununterbrochen (stündlich)**.

Bei Verwenden des Synchronisierungsmodus **Fast ununterbrochen (stündlich)** wird die Netzwerkauslastung auf den ganzen Tag verteilt. Wird die Synchronisierung **Nur vor dem Erstellen der Schattenkopie** durchgeführt, führt dies unter Umständen zu erhöhtem Netzwerkverkehr, jedoch werden nicht den ganzen Tag Daten gesendet.

Wenn in einer Organisation die Netzwerkbandbreite zwischen dem Dateiserver und dem DPM-Server eingeschränkt wird, und wenn diese eingeschränkte Bandbreite sowohl für Sicherungsvorgänge als auch für normale Geschäftsnutzung verwendet werden soll, wird empfohlen, die Synchronisierung nur vor Durchführung von Schattenkopien außerhalb der Hauptgeschäftszeiten zu planen.

Obwohl die Auswirkungen auf Netzwerkverkehr und Netzwerkleistung von Bedeutung sind, müssen Sie auch berücksichtigen, welchen Einfluss die einzelnen Synchronisierungsmodi auf die Wiederherstellung von Daten haben. Wenn Sie nur einmal am Tag eine Synchronisierung vornehmen, können bis zu 24 Stunden an Daten verloren gehen. Bei einer stündlichen Synchronisierung können jedoch nur Daten verloren gehen, die maximal eine Stunde alt sind.

Planen von Konsistenzprüfungen

Da Konsistenzprüfungen sowohl die Leistung des DPM-Servers als auch des Dateiservers beeinträchtigen, sollten Sie diese zu Zeiten planen, in denen eine verringerte Reaktionszeit des Dateiservers die wenigsten Auswirkungen auf Geschäftsvorgänge hat und der wenigste Netzwerkverkehr zu erwarten ist.

Wenn Sie eine Schutzgruppe erstellen, wird bei der Replikaterstellung automatisch eine Konsistenzprüfung durchgeführt. Nachdem eine Schutzgruppe erstellt wurde, und aufgrund eines Netzwerkausfalls, einem Überlauf des Synchronisierungsprotokolls oder aus einem anderen Grund ein inkonsistentes Replikat vorhanden ist, können Sie eine manuelle Konsistenzprüfung durchführen. Eine Anleitung hierzu finden Sie in der DPM-Hilfe unter „How to synchronize a replica“ (http://go.microsoft.com/fwlink/?linkid=51910, in englischer Sprache).

Sie können auch eine tägliche Konsistenzprüfung planen, um sicherzustellen, dass inkonsistente Replikate automatisch repariert werden. Eine geplante Konsistenzprüfung wird nur ausgeführt, wenn ein inkonsistentes Replikat vorhanden ist. Sie könnten beispielsweise am Sonntag die Schutzgruppenoptionen ändern, um eine tägliche Konsistenzprüfung zu planen. Von Sonntag bis Mittwoch werden Datenschutzaufträge erfolgreich abgeschlossen und alle Replikate erfolgreich synchronisiert. Aus diesem Grund wird die tägliche Konsistenzprüfung nicht ausgeführt, da alle Replikate konsistent sind. Am Donnerstag wird dann eine große Anzahl neuer Dateien auf einen geschützten Dateiserver kopiert, und für das Synchronisierungsprotokoll auf dem Dateiserver steht nicht mehr genügend Speicherplatz zur Verfügung. Bei der nächsten regulären Synchronisierung tritt ein Fehler auf, von DPM wird eine "Replikat inkonsistent"-Warnung ausgegeben, und die betroffenen Replikate werden als inkonsistent gekennzeichnet. Da Sie eine Konsistenzprüfung geplant haben, führt DPM zum geplanten Zeitpunkt eine Konsistenzprüfung durch und repariert die Replikate.

In den Planungsoptionen können Sie eine Zeitdauer oder Zeitspanne konfigurieren, in denen Konsistenzprüfungsaufträge ausgeführt werden. Sie können den Beginn der Konsistenzprüfung beispielsweise auf 20:00 Uhr festlegen, wenn die meisten Mitarbeiter des Unternehmens nicht mehr im Haus sind, und eine maximale Dauer von 10 Stunden angeben. Wenn die Konsistenzprüfung nach Ablauf der 10 Stunden nicht fertig gestellt ist, wird diese am nächsten Tag um 6:00 Uhr von DPM angehalten. Um 20:00 Uhr wird der Konsistenzprüfungsauftrag von DPM fortgesetzt. Auf diese Weise wird die Konsistenzprüfung jeden Tag angehalten und wieder

fortgesetzt, bis der Konsistenzprüfungsauftrag erfolgreich abgeschlossen wurde. Eine Anleitung zum Planen einer täglichen Konsistenzprüfung finden Sie in der DPM-Hilfe unter „How to modify protection options“ (http://go.microsoft.com/fwlink/?linkid=51911, in englischer Sprache).

Hinweis

Eine angehaltene Konsistenzprüfung wird im Aufgabenbereich **Überwachung** als **Abgebrochen** angezeigt.

Informationen zu Planungsüberlegungen für den Fall, dass sich der DPM-Server und der geschützte Dateiserver in verschiedenen Zeitzonen befinden, finden Sie in diesem Handbuch im Kapitel „Verwalten von Servern“ (http://go.microsoft.com/fwlink/?LinkId=46367).

Manuelles Erstellen von Replikaten

Beim Erstellen einer Schutzgruppe können Sie auswählen, ob Replikate manuell von Band oder anderen Wechselmedien erstellt werden, um so die Auslastung von Dateiservern und dem Netzwerk zu verringern.

Die automatische Replikaterstellung ist einfacher, in Abhängigkeit von der Größe der geschützten Daten kann die manuelle Replikaterstellung jedoch schneller sein. Bei kleineren Datasets wird die automatische Erstellung empfohlen. Für große Datasets und langsame Netzwerke ist die manuelle Option wahrscheinlich die bessere Wahl.

Nachdem das Replikat erstellt wurde, müssen Sie eine Synchronisierung mit Konsistenzprüfung ausführen.

Eine Anleitung zum manuellen Erstellen eines Replikats finden Sie in der DPM-Hilfe in „Choose Replica Creation Method“ (http://go.microsoft.com/fwlink/?LinkId=51912, in englischer Sprache).

Erhöhen der Kapazität

Sie können die Leistung auch steigern, indem Sie die Kapazität des DPM-Servers durch Hardwareaktualisierungen erhöhen.

- **Durch Hinzufügen von Datenträgern zum Speicherpool** und Neuzuweisung der Replikate im Speicherpool kann die Warteschlangenlänge der Datenträger verringert werden.
- **Eine Erweiterung des Arbeitsspeichers** ist eine vergleichsweise kostengünstige Aktualisierung, die zu einer spürbaren Verbesserung der Leistung führt, wenn der Server häufig über wenig freien Arbeitsspeicher verfügt.
- **Durch Hinzufügen weiterer Prozessoren oder Aktualisieren auf schnellere Prozessoren** können einige CPU-Probleme vermieden werden.

Berücksichtigen Sie außerdem die Datenschutzanforderungen: Möglicherweise müssen Sie zusätzliche DPM-Server einsetzen, um die Arbeitsauslastung auszugleichen.

Empfehlungen zum Optimieren der Leistung des DPM-Servers finden Sie im Kapitel „Planen einer Bereitstellung“ im Planungs- und Bereitstellungshandbuch von DPM 2006 (http://go.microsoft.com/fwlink/?LinkId=46355, in englischer Sprache).

Verwalten der Leistung von DPM in einem WAN

Überlegungen hinsichtlich der Leistung sind eine ernstzunehmende Angelegenheit, wenn der DPM-Server und die entsprechenden geschützten Dateiserver über langsame WAN-Links miteinander verbunden sind. Das gilt insbesondere für Aufträge wie Replikaterstellungen oder Konsistenzprüfungen, die viele Ressourcen benötigen. Beispielsweise würde es 120 Stunden dauern, ein Volume von 20 GB über einen Link mit einer Verbindungsgeschwindigkeit von 512 Kbit/s zu übertragen.

Bei dieser Netzwerkkonfiguration sollten Sie die Komprimierung für alle Schutzgruppen aktivieren. Es wird empfohlen, Replikate von Volumes, die größer sind als 5 GB, manuell zu erstellen.

Eine Replikaterstellung kann nicht in derselben Weise unterbrochen und fortgesetzt werden wie eine Konsistenzprüfung. Wenn eine manuelle Replikaterstellung nicht möglich oder praktikabel ist, und wenn wegen geschäftlicher Anforderungen in gegebener Zeit kein Replikat über das Netzwerk erstellt werden kann, bietet der folgende Ansatz einen Ausweg:

1. Erstellen Sie die Schutzgruppe, und legen Sie fest, dass DPM das Replikat automatisch über das Netzwerk erstellt.
2. Während die Replikaterstellung für die Schutzgruppe durchgeführt wird, brechen Sie den Vorgang ab.
3. Planen Sie eine regelmäßige Konsistenzprüfung, und geben Sie dabei ein Aktivitätsfenster an, durch dass keine täglichen Vorgänge oder die Netzwerkleistung beeinträchtigt werden.

DPM erstellt die Replikate dann während der Konsistenzprüfung. Wenn Sie auf diese Weise vorgehen, werden Daten langsamer übertragen als während der Replikaterstellung. Die Konsistenzprüfung wird jedoch nur zu den konfigurierten Zeiten fortgesetzt, bis diese abgeschlossen ist.

KAPITEL 4

Verwalten von Servern

Als Systemadministrator verwalten Sie Server gewöhnlich in verschiedenen Rollen. Wartungsroutinen werden für jede Serverrolle entsprechend geplant, und diese Rolle wird bei strukturellen Änderungen berücksichtigt, z. B. bei Änderungen des Servernamens oder des Serverstandorts. Was müssen Sie also beachten, wenn die Rollen von DPM-Servern und geschützten Dateiservern der Netzwerkstruktur hinzugefügt werden?

In diesem Kapitel werden die häufigsten Wartungsaufgaben unter Windows und deren Verwendung für DPM-Server und geschützte Dateiserver beschrieben. Es wird ein Leitfaden zum Ändern von Serverkonfigurationen nach dem Einrichten von DPM bereitgestellt, sowie nützliche Informationen zum Konfigurieren von Dateiservern, die sich in einer anderen Zeitzone als der DPM-Server befinden. Darüber hinaus werden in diesem Kapitel Informationen zum Konfigurieren von Firewalls auf dem DPM-Server und den entsprechenden geschützten Dateiservern bereitgestellt, sodass die Kommunikation zwischen diesen Servern gewährleistet bleibt.

In diesem Kapitel

Durchführen allgemeiner Serverwartung

- Verwenden von Windows-Wartungstools
- Aktualisieren des Betriebssystems
- Ausführen von Antivirusprogrammen
- Sichern von Servern

Verwalten des DPM-Servers

- Suchen von DPM-Servern in Active Directory
- Hinzufügen von Datenträgern zum DPM-Server
- Verschieben des DPM-Servers zwischen Domänen
- Ändern der Zeitzone des DPM-Servers
- Neu starten des DPM-Servers

Verwalten von Dateiservern

- Verschieben von Dateiservern zwischen Domänen
- Umbenennen eines Dateiservers
- Wiederherstellen des Schutzes auf einem Dateiserver nach Laufwerkfehler oder Datenträgeraktualisierung
- Ausführen von Bildschirmschonern auf Dateiservern
- Ändern der Zeitzone von Dateiservern

Koordinieren des Schutzes zwischen Zeitzonen

- Anzeige von Zeiten in DPM
- Planen der ersten Replikaterstellung
- Sommer-/Winterzeit in DPM

Konfigurieren von Firewalls
Protokolle und Ports
Wann ein Konfigurieren der Firewall erforderlich ist
Konfigurieren einer Firewall auf einem DPM-Server
Konfigurieren einer Firewall auf einem Dateiserver

Durchführen allgemeiner Serverwartung

Zur allgemeinen Serverwartung zählen Aufgaben wie Datenträger- oder Dateiverwaltung, Aktualisierung von Betriebssystemen und Anwendungen sowie Datenschutz unter Verwendung von Antivirusprogrammen und regelmäßiger Sicherungen. Beim Warten von DPM-Servern und Dateiservern sind einige Besonderheiten zu berücksichtigen.

Folgende Themen werden in diesem Abschnitt behandelt:

• Verwenden von Windows-Wartungstools

• Aktualisieren des Betriebssystems

• Ausführen von Antivirusprogrammen

• Sichern von Servern

Verwenden von Windows-Wartungstools

Im Allgemeinen können Sie den DPM-Server und geschützte Dateiserver dem regulären Wartungsplan hinzufügen und die mit Windows Server 2003 bereitgestellten Wartungstools verwenden. Sie müssen jedoch bei einigen Tools ein paar Besonderheiten beachten, wenn Sie diese mit DPM verwenden. Diese Tools werden in Tabelle 4.1 aufgeführt.

Tabelle 4.1 Windows-Wartungstools und DPM

Windows-Tool	Besonderheiten
Datenträgerbereinigung: Dient dem Entfernen temporärer Dateien, Dateien im Internetcache und nicht erforderlicher Programmdateien	Die Datenträgerbereinigung steht für Replikatvolumes im DPM-Speicherpool nicht zur Verfügung.
Datenträgerdefragmentierung: Dient dem Analysieren der Fragmentierung von Volumes und dem Defragmentieren von Volumes	Bevor Sie einer Schutzgruppe ein Volume hinzufügen, überprüfen Sie die Fragmentierung des Volumes und defragmentieren Sie das Volume gegebenenfalls mithilfe der Datenträgerdefragmentierung. Wenn extrem fragmentierte Volumes geschützt werden, kann unter Umständen der Zeitaufwand zum Neustart von Dateiservern erhöht werden, und Schutzaufträge können möglicherweise fehlschlagen.

	Es wird empfohlen, vor der Datenträgerdefragmentierung die Datenträgerbereinigung auszuführen.
Chkdsk.exe: Dient der Fehlerüberprüfung des Dateisystems und der Dateisystemmetadaten sowie dem Anzeigen eines entsprechenden Statusberichts	Bevor Sie für ein geschütztes Volume **Chkdsk /f** ausführen, stellen Sie sicher, dass für das Volume gerade keine Konsistenzprüfung durchgeführt wird. Wenn Sie für ein geschütztes Volume **Chkdsk /f** während einer Konsistenzprüfung ausführen, kann dies zu einer CPU-Auslastung von 100 % führen. Führen Sie eine Synchronisierung mit Konsistenzprüfung aus, nachdem Sie auf dem Dateiserver Chkdsk.exe ausgeführt haben.

Aktualisieren des Betriebssystems

Ein wichtiger Teil der Computerwartung ist es, sicherzustellen, dass Betriebssysteme und Software auf dem neuesten Stand sind. Aktualisierungen, „Updates“, „Patches“, „Service Packs“ und „Rollups“ genannt, dienen dem Schutz von Computern und Daten.

Sie können sowohl für DPM-Server als auch geschützte Dateiserver die von Ihnen bevorzugte Methode zum Bereitstellen von Softwareupdates verwenden, z. B. Automatische Updates oder Windows Update Services (früher Software Update Services 2.0). Da für manche Softwareupdates ein Neustart des Computers erforderlich ist, sollten Sie diese Aktualisierungen planen oder zu Zeiten durchführen, in denen die wenigsten Auswirkungen auf Datenschutzvorgänge zu erwarten sind.

Hinweis

Wenn Sie einen geschützten Dateiserver auf Windows Server 2003 Service Pack 1 aktualisieren, müssen Sie auch den DPM-Datei-Agent aktualisieren. Anweisungen zum Aktualisieren von Datei-Agents finden Sie unter „How to install a file agent“ (http://go.microsoft.com/fwlink/?LinkId=51988, in englischer Sprache) in der DPM-Hilfe.

Darüber hinaus sollten Sie regelmäßig überprüfen, ob Aktualisierungen von DPM und von Software, die für DPM erforderlich ist, vorhanden sind. Die folgenden Anwendungen sind für DPM erforderlich:

• Internetinformationsdienste 6.0 (IIS – Internet Information Services)

• Microsoft SQL Server™ 2000 (Standard Edition oder Enterprise Edition)

- Microsoft SQL Server™ 2000 Service Pack 3a (SP3a) oder höher
- Microsoft SQL Server™ 2000-Hotfix 859
- Microsoft SQL Server™ 2000 Reporting Services (Standard Edition oder Enterprise Edition)
- Microsoft SQL Server™ 2000 Reporting Services Service Pack 1 (SP1) oder höher

Ausführen von Antivirusprogrammen

DPM ist mit den meisten verbreiteten Antivirusprogrammen kompatibel. Allerdings kann die Leistung von DPM durch Antivirusprogramme beeinträchtigt werden. Fehlerhafte Einstellungen können sogar Beschädigungen von Daten in Replikaten und Schattenkopien verursachen. Führen Sie folgende Schritte aus, um diese Probleme zu verringern:

- **Deaktivieren Sie die Echtzeitüberwachung von Msdpmfsagent.exe auf dem DPM-Server**

  Zum Minimieren der Leistungsbeeinträchtigung deaktivieren Sie im Antivirusprogramm für alle geschützten Volumes die Echtzeitüberwachung der Replikate und Übertragungsprotokolle, indem Sie die Echtzeitüberwachung des DPM-Prozesses **msdpmfsagent.exe** im Ordner **Programme\Microsoft Data Protection Manager\DPM\bin** deaktivieren.

  Bei Echtzeitüberprüfung von Replikaten und Übertragungsprotokollen scannt das Antivirusprogramm bei jeder Synchronisierung von DPM mit dem Dateiserver die Übertragungsprotokolle sowie alle betroffenen Dateien bei Änderungen, die DPM an den Replikaten vornimmt. Dieser Vorgang beeinträchtigt die Leistung von DPM. Wenn Sie diese Funktion für Replikate und Übertragungsprotokolle deaktivieren, ist das Problem jedoch behoben. Eine Anleitung zum Konfigurieren der Echtzeitüberwachung auf Grundlage von Prozessnamen finden Sie im Produkthandbuch des Antivirusprogramms.

  Hinweis

  Antivirusprogramme von McAfee überprüfen nur die ersten 15 Zeichen eines Prozessnamens. Geben Sie als Prozessnamen also **Msdpmfsagent.ex** anstatt **Msdpmfsagent.exe** an, um die Echtzeitüberwachung von **Msdpmfsagent.exe** für Antivirusprogramme von McAfee zu deaktivieren.

- **Deaktivieren Sie die Echtzeitüberwachung von Csc.exe auf dem DPM-Server**

  Wenn die Leistung der DPM-Verwaltungskonsole beeinträchtigt wird, deaktivieren Sie zusätzlich die Echtzeitüberwachung des Prozesses **csc.exe**, der sich im Ordner **%windir%\microsoft.net\framework\v1.1.4322\csc.exe** befindet. Der Prozess **csc.exe** ist der C#-Compiler. Die Leistung wird durch Echtzeitüberwachung des Prozesses **csc.exe** beeinträchtigt, da das Antivirusprogramm Dateien überprüft, die durch den Prozess **csc.exe** beim Erstellen von XML-Nachrichten ausgegeben werden. Eine Anleitung zum Konfigurieren der Echtzeitüberwachung auf Grundlage von Prozessnamen finden Sie im Produkthandbuch des Antivirusprogramms.

- **Löschen Sie infizierte Dateien auf den Dateiservern und dem DPM-Server**

  Um Datenbeschädigung in Replikaten und Schattenkopien zu verhindern, konfigurieren Sie das Antivirusprogramm so, dass infizierte Dateien gelöscht anstatt automatisch bereinigt oder in ein Quarantäneverzeichnis verschoben werden. Das automatische Bereinigen oder Verschieben von Dateien in ein Quarantäneverzeichnis kann zu Datenbeschädigungen führen, da das Antivirusprogramm bei diesen Vorgängen Änderungen an Dateien vornimmt, die von DPM nicht erkannt werden.

Wenn DPM versucht, ein Replikat zu synchronisieren, das von einem anderen Programm geändert wurde, können Datenbeschädigungen in dem Replikat und den Schattenkopien verursacht werden. Beheben Sie dieses Problem, indem Sie das Antivirusprogramm so konfigurieren, dass infizierte Dateien gelöscht werden. Eine Anleitung zum Konfigurieren des Antivirusprogramms zum Löschen infizierter Dateien finden Sie im Produkthandbuch des Antivirusprogramms.

Wichtig

Jedes Mal, wenn das Antivirusprogramm eine Datei des Replikats löscht, muss ein Konsistenzprüfungsauftrag ausgeführt werden, auch wenn das Replikat nicht als inkonsistent gekennzeichnet wird.

Sichern von Servern

Es wird empfohlen, regelmäßige Sicherungskopien der Server zu erstellen. Die Aufgabe von DPM ist das Sichern und Wiederherstellen von Daten der Dateiserver. DPM kann jedoch weder sich selbst noch die Betriebssysteme und Anwendungen der Dateiserver schützen. Für ein vollständiges Wiederherstellen eines DPM- oder Dateiservers ist eine Archivierung des Systemstatus erforderlich. Eine Methode zum Archivieren des Systemstatus ist das Verwenden von Backup, der Sicherungssoftware in Windows Server 2003.

Mit Backup können Sie einen automatischen Systemwiederherstellungssatz (ASR – Automated System Recovery) erstellen. Der automatische Systemwiederherstellungssatz beinhaltet eine Sicherungskopie des Systemstatus, der Systemdienste und sämtlicher Festplatten, die den Betriebssystemkomponenten zugeordnet sind. Im Satz ist außerdem ein Startdatenträger mit Informationen über die Sicherungskopie und die Festplattenkonfigurationen enthalten. Erstellen Sie regelmäßig und vor allem nach umfassenden Systemänderungen einen neuen automatischen Systemwiederherstellungssatz.

Eine schrittweise Anleitung für das Wiederherstellen von Systemstatus auf DPM- und Dateiservern mithilfe der automatischen Systemwiederherstellung finden Sie im Whitepaper „Using Data Protection Manager and Windows Backup“ (http://go.microsoft.com/fwlink/?linkid=47057, in englischer Sprache).

Warnung

Es ist wichtig, dass Sie Sicherungskopien der DPM-Servervolumes erstellen, auf denen die Systemdateien für DPM, SQL Server und SQL Server Reporting Services enthalten sind. Wenn in einem Notfall nur einige der von DPM benötigten Dateien verloren gehen, müssen Sie die Volumes mithilfe der erforderlichen Dateien wiederherstellen, bevor DPM installiert oder deinstalliert werden kann.

Weitere Informationen über das Archivieren und Wiederherstellen von Daten auf DPM- und Dateiservern finden Sie im Kapitel „Archivieren und Wiederherstellen von Daten“ (http://go.microsoft.com/fwlink/?LinkId=46368) in diesem Handbuch.

Verwalten des DPM-Servers

In diesem Abschnitt finden Sie Informationen zum Ausführen folgender Aufgaben:

• Suchen von DPM-Servern in Active Directory

• Hinzufügen von Datenträgern zum DPM-Server

- Verschieben des DPM-Servers zwischen Domänen
- Ändern der Zeitzone des DPM-Servers
- Neu starten des DPM-Servers

Suchen von DPM-Servern in Active Directory

Mithilfe von Active Directory können von Benutzern oder Programmen Informationen über Verzeichnisobjekte abgefragt werden. Beim Installieren von DPM auf einem Mitgliedsserver einer Domäne wird in Active Directory ein Dienstverbindungspunkt registriert. Mit den Informationen, die mit dem Dienstverbindungspunkt registriert werden, können Sie in Active Directory nach Computern suchen, auf denen DPM ausgeführt wird.

Hinweis

Wird DPM auf einem Server installiert, der nicht Mitglied einer Domäne ist, und wird dieser Server anschließend einer Domäne hinzugefügt, so wird der Dienstverbindungspunkt nicht in Active Directory registriert.

Um in Active Directory nach DPM-Servern zu suchen, verwenden Sie ein Active Directory-Abfragetool wie z. B. ADSIEdit, mit dem Sie nach allen Computern in der Domäne suchen können, die über einen Dienstverbindungspunkt **serviceClassName=MSDPM** verfügen.

ADSIEdit ist ein Microsoft Management Console-Snap-In, das mit den Windows Server 2003-Supporttools installiert wird.

So installieren Sie Windows Server 2003-Supporttools

1. Legen Sie die Windows Server 2003-CD ein.
2. Wechseln Sie in das Verzeichnis **\Support\Tools**.
3. Doppelklicken Sie auf den Dateinamen **suptools.msi**.

So suchen Sie mithilfe von ADSIEdit nach DPM-Servern

1. Führen Sie die Datei **adsiedit.msc** aus.
2. Klicken Sie mit der rechten Maustaste auf den Knoten **Domäne**, zeigen Sie auf **Neu**, und klicken Sie anschließend auf **Abfrage**.
3. Geben Sie einen Namen für die Abfrage ein, z. B. **MSDPM-Server**.
4. Wählen Sie den Knoten **Computer** als Stamm der Suche aus.
5. Geben Sie unter **Abfragezeichenfolge:** die Zeichenfolge **serviceClassName=MSDPM** ein.
6. Klicken Sie auf **OK**.

   Unter dem Knoten **Domäne** wird ein Knoten für die Abfrage angezeigt.
7. Wählen Sie den Abfrageknoten aus.

   Im Listenbereich werden die Server angezeigt, auf denen DPM installiert ist.

Weitere Informationen über das Verwenden von ADSIEdit finden Sie im Artikel „Adsiedit Overview“ im Microsoft Windows Server 2003 TechCenter (http://go.microsoft.com/fwlink/?LinkId=50377, in englischer Sprache).

Hinzufügen von Datenträgern zum DPM-Server

Wenn Sie dem Speicherpool einen Datenträger hinzufügen, wird der Datenträger von DPM neu formatiert. Durch diesen Vorgang werden alle Daten des Datenträgers gelöscht. Wenn es sich bei dem neuen Datenträger um eine Basisfestplatte handelt, wandelt DPM den Datenträger in einen dynamischen Datenträger um. In einigen Fällen können beim Umwandeln zu einem dynamischen Datenträger Fehler auftreten, vor allem, wenn bereits große Volumes auf der Basisfestplatte vorhanden sind. Verwenden Sie bei Auftreten eines Fehlers die Datenträgerverwaltung von Windows, um sämtliche Volumes auf der Basisfestplatte zu löschen, und fügen Sie anschließend den Datenträger dem DPM-Speicherpool hinzu.

Wenn der Name eines Datenträgers im Aufgabenbereich **Verwaltung** der DPM-Verwaltungskonsole auf der Registerkarte **Datenträger** als **Unbekannt** angezeigt wird, kann der Datenträger erst dem Speicherpool hinzugefügt werden, wenn der Datenträgername korrigiert wurde. Gehen Sie folgendermaßen vor, um das Problem zu lösen:

So korrigieren Sie einen Datenträgernamen

1. Erweitern Sie im **Geräte-Manager** den Knoten **Laufwerke**.
2. Klicken Sie mit der rechten Maustaste auf jeden Datenträger, der als **Datenträger** aufgeführt wird, und wählen Sie **Deinstallieren** aus.

   Alle Datenträger ohne Anzeigenamen werden als **Datenträger** angezeigt. Ein Anzeigename ist z. B. „HITACHI_DK23EB-40“.
3. Klicken Sie im Menü **Aktion** auf **Nach geänderter Hardware suchen**, um den Datenträger neu zu installieren.

Weitere Informationen finden Sie unter „Managing Disks“ (http://go.microsoft.com/fwlink/?LinkId=51975, in englischer Sprache) in der DPM-Hilfe.

Verschieben des DPM-Servers zwischen Domänen

DPM bietet nur für Dateiserver Schutz, die sich innerhalb der gleichen Domäne befinden. Wenn Sie einen DPM-Server in eine andere Domäne verschieben, besteht kein Schutz mehr für die Dateiserver, die in der ursprünglichen Domäne bleiben. Sie können jedoch folgende Schritte ausführen:

- Einen DPM-Server in eine andere Domäne verschieben, um die Dateiserver in dieser Domäne zu schützen.
- Einen DPM-Server und die von diesem geschützten Dateiserver in eine andere Domäne verschieben.

So verschieben Sie nur den DPM-Server in eine andere Domäne

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.
2. Deinstallieren Sie sämtliche Datei-Agents auf den Dateiservern.
3. Verschieben Sie den DPM-Server in die neue Domäne.
4. Installieren Sie Datei-Agents auf den Dateiservern der neuen Domäne.
5. Konfigurieren Sie neue Schutzgruppen, die Dateiserver der neuen Domäne enthalten.

So verschieben Sie den DPM-Server und die geschützten Dateiserver in eine andere Domäne

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen, behalten Sie jedoch die Replikate und Schattenkopien bei.
2. Deinstallieren Sie sämtliche Datei-Agents auf den Dateiservern.
3. Verschieben Sie den DPM-Server und die Dateiserver in die neue Domäne.
4. Installieren Sie Datei-Agents auf den zuvor geschützten Dateiservern.
5. Konfigurieren Sie die vorherigen Schutzgruppen neu, um die zuvor geschützten Daten erneut zu schützen.

   DPM weist jedem Mitglied der Schutzgruppe die entsprechenden Replikate der ursprünglichen Domäne zu.

Sollte das Verschieben des DPM-Servers das Ändern der Zeitzonenkonfiguration auf diesem Server erfordern, finden Sie im folgenden Abschnitt, „Ändern der Zeitzone des DPM-Servers“, eine Anleitung für diese Aufgabe.

Ändern der Zeitzone des DPM-Servers

Führen Sie folgende Schritte aus, um die Zeitzone des DPM-Servers zu ändern.

So ändern Sie die Zeitzone des DPM-Servers

1. Schließen Sie die DPM-Verwaltungskonsole.
2. Halten Sie den DPM-Dienst an (**MsDpm.exe**).
3. Ändern Sie die Zeitzone des DPM-Servers in der Systemsteuerung mithilfe der Registerkarte **Zeitzone** im Dialogfeld **Eigenschaften von Datum und Uhrzeit**.
4. Öffnen Sie die DPM-Verwaltungskonsole.

   Durch diese Aktion wird auch der DPM-Dienst erneut gestartet.
5. Klicken Sie in der DPM-Verwaltungskonsole im Menü **Aktion** auf **Optionen**.
6. Klicken Sie im Dialogfeld **Optionen** auf die Registerkarte **AutoErmittlung**, ändern Sie die Zeit für die automatische Erkennung, und klicken Sie auf **OK**.

   Durch das Ändern des Zeitplans für die automatische Erkennung werden alle DPM-Aufträge entsprechend der neuen Zeitzone des DPM-Servers neu erstellt.

Weitere Informationen zu Zeitzonen finden Sie im Abschnitt „Koordinieren des Schutzes zwischen Zeitzonen“ in diesem Kapitel.

Neu starten des DPM-Servers

Sollte ein Neustart des DPM-Servers notwendig sein, überprüfen Sie in der DPM-Verwaltungskonsole im Aufgabenbereich **Überwachung**, ob zurzeit Aufträge durchgeführt werden, und befolgen Sie diese Richtlinien:

- Wenn keine Aufträge ausgeführt werden oder für die Zeit geplant sind, die für den Neustart erforderlich ist, starten Sie den DPM-Server neu.
- Wenn eine Synchronisierung mit einem Konsistenzprüfungsauftrag ausgeführt wird, starten Sie den DPM-Server neu. Die Synchronisierung mit Konsistenzprüfung wird zum nächsten geplanten Zeitpunkt fortgesetzt. Sie können den Auftrag auch manuell neu starten.
- Wenn ein Replikaterstellungsauftrag ausgeführt wird, verschieben Sie den Neustart, bis der Auftrag abgeschlossen ist. Wenn der Neustart nicht verschoben werden kann, müssen Sie nach dem Neustart des DPM-Servers die Synchronisierung mit Konsistenzprüfung für das Replikat manuell ausführen.
- Wenn das Erstellen von Schattenkopien oder deren Synchronisierung für die Zeit des Neustarts geplant ist, verschieben Sie den Neustart, bis die Schattenkopien erstellt sind, oder führen Sie nach dem Neustart des DPM-Servers die Synchronisierungen und das Erstellen der Schattenkopien manuell aus.

Verwalten von Dateiservern

Verschiedene Ereignisse oder Geschäftsanforderungen können Änderungen an den geschützten Dateiservern erforderlich machen. In diesem Abschnitt finden Sie Informationen darüber, wie Sie folgende Änderungen vornehmen können:

- Verschieben von Dateiservern zwischen Domänen
- Umbenennen eines Dateiservers
- Wiederherstellen des Schutzes auf einem Dateiserver nach Laufwerkfehler oder Datenträgeraktualisierung
- Ausführen von Bildschirmschonern auf Dateiservern
- Ändern der Zeitzone von Dateiservern

Verschieben von Dateiservern zwischen Domänen

DPM bietet nur für Dateiserver Schutz, die sich innerhalb der gleichen Domäne befinden. Wenn Sie einen Dateiserver in eine andere Domäne verschieben, besteht kein Schutz mehr durch den DPM-Server, der in der ursprünglichen Domäne bleibt. Sie können jedoch folgende Schritte ausführen:

- Den Dateiserver in eine andere Domäne verschieben und diesen mithilfe eines DPM-Servers in der neuen Domäne schützen.
- Einen DPM-Server und die von diesem geschützten Dateiserver in eine andere Domäne verschieben.

So verschieben Sie nur den Dateiserver in eine andere Domäne

1. Entfernen Sie alle Mitglieder des Dateiservers aus den Schutzgruppen.
2. Deinstallieren Sie den Datei-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Verschieben Sie den Dateiserver in die neue Domäne.
4. Installieren Sie einen Datei-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server der neuen Domäne.
5. Fügen Sie die Volumes oder Freigaben des Dateiservers zu den Schutzgruppen des DPM-Servers in der neuen Domäne hinzu.

Sollte das Verschieben des Dateiservers das Ändern der Zeitzonenkonfiguration auf diesem Server erfordern, finden Sie im Abschnitt „Ändern der Zeitzone von Dateiservern“ in diesem Kapitel eine Anleitung für diese Aufgabe.

Umbenennen eines Dateiservers

DPM verwendet den Namen des Dateiservers als eindeutigen Bezeichner für Replikate, Schattenkopien, DPM-Datenbankeinträge, Berichtsdatenbankeinträge usw.

Folgende Aktionen können nicht durchgeführt werden:

- Umbenennen eines geschützten Dateiservers ohne Unterbrechung des Serverschutzes.
- Umbenennen eines geschützten Dateiservers und Zuordnen der bestehenden Replikate und Schattenkopien mithilfe des neuen Dateiservernamens.

Es wird empfohlen, den Namen eines geschützten Dateiservers nicht zu ändern. Um den Namen eines geschützten Dateiservers zu ändern, müssen zwei Aufgaben ausgeführt werden:

- Entfernen des Schutzes des Dateiservers (ursprünglicher Servername).
- Schutz des Dateiservers (neuer Servername).

So ändern Sie den Namen eines Dateiservers

1. Entfernen Sie alle Mitglieder aus den Schutzgruppen.

   Wenn Sie die Replikate und Schattenkopien beibehalten, kann der Administrator weiterhin auf die Daten zur Wiederherstellung zugreifen, bis die Replikate gelöscht werden. Datenzugriff für die Endbenutzerwiederherstellung ist allerdings nicht möglich.

2. Deinstallieren Sie den Datei-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
3. Ändern Sie den Namen des Dateiservers.
4. Installieren Sie einen Datei-Agent mithilfe der DPM-Verwaltungskonsole auf dem DPM-Server.
5. Fügen Sie die Volumes oder Freigaben des Dateiservers zu den Schutzgruppen des DPM-Servers hinzu.

Wiederherstellen des Schutzes auf einem Dateiserver nach Laufwerkfehler oder Datenträgeraktualisierung

In verschiedenen Situationen kann es erforderlich sein, Daten von Band wiederherzustellen, z. B. bei einem Datenträgerfehler, einer Datenträgeraktualisierung oder Änderungen der GUID (Globally Unique Identifier) des geschützten Dateiservervolumes. Wenn Sie einen Datenträger ersetzen, wird jedem Volume auf dem neuen Datenträger eine neue GUID zugewiesen. Auch wenn Sie dem neuen Volume den gleichen Laufwerksbuchstaben des Volumes auf dem alten Datenträger zuweisen, erkennt DPM die neue GUID nicht. DPM erkennt die Änderung der Mitgliedschaft und erstellt während des nächsten Synchronisierungsauftrags eine Warnung. Das Replikat für jedes Volume des alten Datenträgers wird als inkonsistent gekennzeichnet.

So stellen Sie die Daten auf den Volumes der neuen Datenträger wieder her und aktivieren den Schutz für die wiederhergestellten Volumes

1. Sichern Sie das Replikat der alten Volumes des DPM-Servers auf Band, wenn noch keine Sicherungskopien der Replikate für jedes Volume vorhanden sind.

   Hinweis

   Eine Anleitung für das Sichern von Replikaten finden Sie im Kapitel „Archivieren und Wiederherstellen von Daten“ in diesem Handbuch (http://go.microsoft.com/fwlink/?LinkId=46368).

2. Stellen Sie die Daten von jedem der ursprünglichen Volumes auf einem neuen Volume mit einer der folgenden Methoden wieder her:

   - Verwenden Sie den Aufgabenbereich **Wiederherstellung** in der DPM-Verwaltungskonsole, um Daten einer Schattenkopie des ursprünglichen Volumes auf dem neuen Volume durch Ändern des Wiederherstellungsziels wiederherzustellen.
   - Wenn eine Sicherungskopie des ursprünglichen Volumes des Dateiservers auf Band vorhanden ist, stellen Sie die Daten auf dem neuen Volume des Dateiservers mithilfe der Bandsicherungskopie wieder her. Eine Anleitung für das Verwenden der Sicherungssoftware finden Sie in der Dokumentation der Sicherungssoftware.
   - Verwenden Sie die Sicherungskopie des Replikats aus Schritt 1, und befolgen Sie die Schritte im Abschnitt „Wiederherstellen von Daten vom Band auf Dateiserver“ im Kapitel „Archivieren und Wiederherstellen von Daten“ in diesem Handbuch (http://go.microsoft.com/fwlink/?LinkId=46368).

3. Entfernen Sie sämtliche Volumes des alten Datenträgers aus ihren Schutzgruppen. Sie können auch auf das Abschließen des nächtlichen Planaktualisierungsauftrags warten, da DPM alle Änderungen in der Schutzkonfiguration erkennt und eine Warnung erstellt. In der Warnung wird für jedes Volume des neuen Datenträgers ein Gruppenmitglied mit der Bezeichnung **Neu** und für jedes Volume des alten Datenträgers ein Gruppenmitglied mit der Bezeichnung **Nicht mehr verfügbar** angezeigt. Es wird empfohlen, den Schutz sämtlicher Volumes des alten Datenträgers zu deaktivieren und den Schutz sämtlicher neuer Volumes zu aktivieren. Sie können sämtliche Replikate und Schattenkopien alter Volumes löschen, wenn diese nicht mehr für Wiederherstellungsvorgänge, wie z. B. Endbenutzerwiederherstellung, benötigt werden.

4. Verwenden Sie den **Assistenten zum Erstellen neuer Schutzgruppen** in der DPM-Verwaltungskonsole, um der Schutzgruppe neue Volumes hinzuzufügen. Wählen Sie für jedes neue Volume, das der Schutzgruppe hinzugefügt werden soll, auf der Seite **Replikaterstellungsmethode auswählen** des Assistenten die Option **Ich werde die Dateien selbst auf Data Protection Manager übertragen** aus.

5. Erstellen Sie für jedes Volume das erste Replikat mithilfe der Sicherungssoftware und der Sicherungskopie des Replikats, die mit Schritt 1 von den alten Volumes erstellt wurde. Da die Sicherungs- und Wiederherstellungshierarchien nicht übereinstimmen, muss auf dem DPM-Server FsPathMerge verwendet werden. Sie können auch eine Bandsicherungskopie des alten Volumes des Dateiservers verwenden. Führen Sie zu diesem Zeitpunkt keine Synchronisierung mit Konsistenzprüfung aus.

   Hinweis

   Weitere Informationen zum Erstellen eines Replikats mithilfe einer Bandsicherungskopie finden Sie im Abschnitt „Behandeln von Problemen beim manuellen Erstellen von Replikaten“ im Kapitel „Problembehandlung“ in diesem Handbuch (http://go.microsoft.com/fwlink/?LinkId=46369). Eine Anleitung für das Verwenden von FsPathmerge auf dem DPM-Server finden Sie im Kapitel „Archivieren und Wiederherstellen von Daten“ in diesem Handbuch (http://go.microsoft.com/fwlink/?LinkId=46368).

6. Erstellen Sie manuell für jedes neue geschützte Volume auf dem DPM-Server eine Schattenkopie.

7. Führen Sie für jedes neue Volume die Synchronisierung mit Konsistenzprüfung aus.

Ausführen von Bildschirmschonern auf Dateiservern

Das Verwenden von Bildschirmschonern kann nach dem Installieren des DPM-Agents und nach dem Neustart des Dateiservers eine Endlosschleife mit der Anzeige des Anmeldebildschirms von Windows verursachen. Deaktivieren Sie den Bildschirmschoner, um dieses Problem zu vermeiden. Eine Anleitung zum Deaktivieren des Bildschirmschoners finden Sie im Microsoft Knowledge Base-Artikel „SO WIRD'S GEMACHT: Ändern des Anmeldebildschirmschoners in Windows“ (http://support.microsoft.com/kb/185348/de).

Ändern der Zeitzone von Dateiservern

DPM erkennt während der Installation des Datei-Agents automatisch die Zeitzone eines geschützten Dateiservers. Wenn ein geschützter Dateiserver nach dem Konfigurieren des Schutzes in eine andere Zeitzone verschoben wird, muss die Computerzeit in der Systemsteuerung mithilfe der Registerkarte **Zeitzone** im Dialogfeld **Datum und Uhrzeit** angepasst werden.

So aktualisieren Sie die Zeitzone in der DPM-Datenbank

1. Deinstallieren Sie auf dem Dateiserver unter **Software** das Programm **Microsoft System Center Data Protection Manager 2006-Datei-Agent**.
2. Klicken Sie auf dem DPM-Server in der DPM-Verwaltungskonsole im Aufgabenbereich **Verwaltung** auf die Registerkarte **Agents**, wählen Sie den Dateiserver aus, und klicken Sie anschließend im Bereich **Aktionen** auf **Informationen aktualisieren**.

   Der Status des Agents wird zu **Fehler** geändert.
3. Klicken Sie im Detailbereich auf **Entferne den Dateiservereintrag auf diesem DPM-Computer**.
4. Installieren Sie den Datei-Agent erneut auf dem Dateiserver. Eine Anleitung für diesen Vorgang finden Sie unter „Managing Disks“ (http://go.microsoft.com/fwlink/?LinkId=51975, in englischer Sprache) in der DPM-Hilfe.
5. Führen Sie die Synchronisierung mit Konsistenzprüfung für jedes geschützte Volume des Dateiservers aus. Eine Anleitung für diesen Vorgang finden Sie unter „Working with Replicas“ (http://go.microsoft.com/fwlink/?LinkId=51977, in englischer Sprache) in der DPM-Hilfe.

Koordinieren des Schutzes zwischen Zeitzonen

In einer Active Directory-Domäne wird die Systemzeit der Server entsprechend der für jeden Server konfigurierten Zeitzone synchronisiert. Wenn jedoch ein DPM-Server Dateiserver schützt, die sich in einer anderen Zeitzone als der DPM-Server befinden, müssen Sie die Zeitunterschiede beim Planen von Aufträgen, Prüfen von Berichten, Verwalten von Warnungen und Ausführen von Datenwiederherstellungen berücksichtigen.

Folgende Themen werden in diesem Abschnitt behandelt:

• Zeitanzeige in DPM

• Planen der ersten Replikaterstellung

• Sommer-/Winterzeit in DPM

Anzeige von Zeiten in DPM

Aufträge zur Synchronisierung und Schattenkopieerstellung werden von DPM automatisch entsprechend der Zeitzone des Dateiservers geplant. In allen anderen Bereichen der DPM-Verwaltungskonsole werden die Systemzeiten entsprechend der Zeitzone des DPM-Servers angezeigt. Zwar werden die Aufträge entsprechend der Zeitzone des Dateiservers geplant, die Startzeiten und die Schattenkopiezeiten der Aufträge werden jedoch in der Zeitzone des DPM-Servers angezeigt.

Angenommen, der DPM-Server befindet sich in Berlin und der Dateiserver in Reykjavik, dessen Zeitzone zwei Stunden hinter der von Berlin liegt. Wenn Sie Synchronisierungs- und Schattenkopieaufträge für 18:00 Uhr planen, werden diese Aufträge um 18:00 Uhr Reykjaviker Zeit ausgeführt, also entsprechend der Zeit des Dateiservers. Wenn jedoch ein Benutzer in Reykjavik eine Datenwiederherstellung in den Zustand von 18:00 Uhr des vorangegangenen Tages anfordert, müssen Sie die Schattenkopien von 20:00 Uhr Berliner Zeit suchen. Denn in der DPM-Wiederherstellungsbenutzeroberfläche werden die Zeiten der Schattenkopien entsprechend der Zeitzone des DPM-Servers angezeigt.

Planen der ersten Replikaterstellung

Das Berücksichtigen der Zeitzonen kann sich beim Planen der ersten Replikaterstellung als recht kompliziert erweisen. Die erste Replikaterstellung wird entsprechend der Zeit auf dem DPM-Server geplant und zum geplanten Zeitpunkt auf dem Dateiserver ausgeführt.

Aufträge zur ersten Replikaterstellung werden mithilfe der Zeit des DPM-Servers geplant; es können keine Aufträge für Zeitpunkte geplant werden, die in der Vergangenheit der DPM-Serverzeit liegen, auch wenn diese Zeitpunkte in der Zukunft der Dateiserverzeit liegen. Im Beispiel des DPM-Servers in Berlin, der einen Dateiserver in Reykjavik schützt, besteht ein Zeitunterschied von zwei Stunden zwischen den beiden Serverzeiten. Aus diesem Grund kann um 9:00 Uhr Berliner Zeit das Ausführen einer ersten Replikaterstellung für den Dateiserver in Reykjavik nicht für 8:00 Uhr Reykjaviker Zeit geplant werden.

Angenommen, der DPM-Server in Berlin schützt außerdem einen Dateiserver in Sofia, dessen Zeitzone eine Stunde vor Berlin liegt. In Berlin kann um 20:00 Uhr ein Auftrag zur ersten Replikaterstellung geplant werden, der um 20:30 Uhr auf dem Dateiserver in Sofia ausgeführt werden soll, da dieser Zeitpunkt für den DPM-Server in der Zukunft liegt. Da es jedoch in Sofia bereits später als 20:30 Uhr ist, wird die erste Replikaterstellung sofort ausgeführt.

Sommer-/Winterzeit in DPM

DPM erkennt während der Installation des Datei-Agents automatisch die Zeitzone eines geschützten Dateiservers. Vorausgesetzt, sowohl der DPM-Server als auch der geschützte Dateiserver befinden sich in Zeitzonen, in denen die gleichen Regelungen für die Sommer- und Winterzeit gelten, berücksichtigt DPM automatisch Beginn und Ende der Sommerzeit. Befinden sich jedoch der DPM-Server und der Dateiserver in Zeitzonen, in denen jeweils unterschiedliche Regelungen für die Sommer- und Winterzeit gelten – z. B. wenn sich der DPM-Server in einer Zeitzone befindet, in der die Zeitumstellung durchgeführt wird, der Dateiserver jedoch nicht – wird die Berücksichtigung des Zeitunterschieds zwischen DPM-Server und Dateiserver gestört.

Um dieses Problem zu lösen, können Sie den DPM-Server zwingen, den Zeitunterschied neu einzustellen, indem Sie die Namen der Schutzgruppen der Dateiserver ändern und anschließend wieder in die vorherigen Namen ändern. Durch diesen Vorgang werden Aufträge für die Schutzgruppen neu erstellt, dadurch wird der Zeitunterschied erneut eingestellt.

Konfigurieren von Firewalls

Wenn die zu schützenden Dateiserver von einer Firewall geschützt werden, müssen Sie die Firewall so konfigurieren, dass die Kommunikation zwischen dem DPM-Server, den zu schützenden Dateiservern und den Domänencontrollern zulässig ist.

Protokolle und Ports

Je nach Netzwerkkonfiguration kann eine Konfiguration der Firewall erforderlich sein, um die Kommunikation zwischen DPM-Server, Dateiservern und Domänencontrollern zu ermöglichen. In Tabelle 4.3 sind als Hilfe für die Firewallkonfiguration ausführliche Informationen über die von DPM verwendeten Protokolle und Ports enthalten.

Tabelle 4.3 Von DPM verwendete Protokolle und Ports

Protokoll	Port	Details
DCOM	135/TCP dynamisch	Das Steuerungsprotokoll von DPM verwendet DCOM. DPM sendet Befehle an den Datei-Agent mithilfe von an den Agent gerichteten DCOM-Aufrufen. Der Datei-Agent reagiert mit DCOM-Aufrufen an den DPM-Server. Der TCP-Port 135 ist der von DCOM zur Auflösung verwendete DCE-Endpunkt. In der Standardeinstellung weist DCOM dynamisch Ports aus dem TCP-Portbereich 1024 bis 65535 zu. Sie können diesen Bereich jedoch mithilfe der Komponentendienste konfigurieren. Weitere Informationen finden Sie im MSDN-Artikel „Using Distributed COM with Firewalls“ (http://go.microsoft.com/fwlink/?LinkId=46088, in englischer Sprache).

TCP	3148/TCP 3149/TCP	Der DPM-Datenkanal basiert auf TCP. Sowohl der DPM- als auch der Dateiserver bauen Verbindungen auf, um DPM-Vorgänge wie Synchronisierung und Wiederherstellung zu aktivieren. DPM kommuniziert mit dem DPM-Agent-Koordinator über den Port 3148 und mit dem Datei-Agent über Port 3149.
DNS	53/UDP	Wird zwischen DPM und dem Domänencontroller sowie zwischen dem Dateiserver und dem Domänencontroller zur Hostnamensauflösung verwendet.
Kerberos	88/UDP 88/TCP	Wird zwischen DPM und dem Domänencontroller sowie zwischen dem Dateiserver und dem Domänencontroller zur Authentifizierung des Verbindungsendpunkts verwendet.
LDAP	389/TCP 389/UDP	Wird zwischen DPM und dem Domänencontroller für Active Directory-Abfragen verwendet.
NetBIOS	137/UDP 138/UDP 139/TCP	Wird zwischen DPM und dem Dateiserver, zwischen DPM und dem Domänencontroller sowie zwischen dem Dateiserver und dem Domänencontroller für diverse Vorgänge verwendet.

Wann ein Konfigurieren der Firewall erforderlich ist

Wenn Windows Firewall auf dem DPM-Server während der Installation von DPM aktiviert ist, wird die Firewall von DPM Setup automatisch konfiguriert. Unter folgenden Umständen müssen Sie die Firewall jedoch selbst konfigurieren:

- Wenn Sie eine andere Firewallsoftware als Windows Firewall verwenden oder wenn Windows Firewall nach dem Installieren von DPM aktiviert wird, müssen Sie die Firewall auf dem DPM-Server konfigurieren.
- Wenn eine Firewall auf dem Dateiserver aktiviert ist, müssen Sie die Firewall vor dem Installieren, Aktualisieren oder Deinstallieren des Datei-Agents deaktivieren und anschließend die Firewall auf dem Dateiserver aktualisieren.

Konfigurieren einer Firewall auf einem DPM-Server

Um eine Firewall auf einem DPM-Server zu konfigurieren, müssen Sie Port 135 für TCP-Datenverkehr öffnen und den DPM-Dienst (Msdpm.exe) sowie den Datei-Agent (Msdpmfsagent.exe) für die Kommunikation durch die Firewall freigeben.

Die folgenden Prozeduren gelten für die Konfiguration von Windows Firewall. Wenn Windows Firewall auf dem DPM-Server während der Installation von DPM aktiviert ist, wird die Firewall von DPM Setup automatisch konfiguriert.

Eine Anleitung für das Konfigurieren anderer Firewallsoftware finden Sie in der entsprechenden Firewalldokumentation.

So konfigurieren Sie Windows Firewall auf einem DPM-Server

1. Klicken Sie in der **Systemsteuerung** auf **Windows Firewall**.
2. Überprüfen Sie auf der Registerkarte **Allgemein**, dass Windows Firewall aktiviert und das Kontrollkästchen **Keine Ausnahmen zulassen** deaktiviert ist.
3. Führen Sie auf der Registerkarte **Ausnahmen** folgende Aufgaben durch:
   - Klicken Sie auf **Programm hinzufügen**, dann auf **Durchsuchen**, und wechseln Sie in das Verzeichnis **Programme/Microsoft Data Protection Manager/DPM/bin**. Wählen Sie **Msdpm.exe** aus, klicken Sie auf **Öffnen** und anschließend auf **OK**.
   - Klicken Sie auf **Programm hinzufügen**, dann auf **Durchsuchen**, und wechseln Sie in das Verzeichnis **Programme/Microsoft Data Protection Manager/DPM/bin**. Wählen Sie **Msdpmfsagent.exe** aus, klicken Sie auf **Öffnen** und anschließend auf **OK**.
   - Klicken Sie auf **Anschluss hinzufügen**, geben Sie im Feld **Name** einen Namen für den Port ein (jeder Name ist zulässig), geben Sie im Feld **Portnummer** den Wert **135** ein, überprüfen Sie, ob **TCP** als Protokoll festgelegt ist, klicken Sie auf **OK**, um das Dialogfeld **Anschluss hinzufügen** zu schließen und erneut auf **OK**, um das Dialogfeld **Windows Firewall** zu schließen.

Konfigurieren einer Firewall auf einem Dateiserver

Um eine Firewall auf einem Dateiserver zu konfigurieren, müssen Sie Port 135 für TCP-Datenverkehr öffnen und den Datei-Agent (Msdpmfsagentca.exe) für die Kommunikation durch die Firewall freigeben.

Um auf einem Dateiserver mit aktivierter Firewall einen Datei-Agent installieren, deinstallieren oder aktualisieren zu können, müssen Sie zuerst die Firewall deaktivieren. Danach können Sie mithilfe der DPM-Verwaltungskonsole einen Datei-Agent installieren, deinstallieren oder aktualisieren und anschließend die Firewall wieder aktivieren.

Die folgenden Prozeduren gelten für die Konfiguration von Windows Firewall. Eine Anleitung für das Konfigurieren anderer Firewallsoftware finden Sie in der entsprechenden Firewalldokumentation.

So deaktivieren Sie Windows Firewall auf einem Dateiserver

1. Klicken Sie in der **Systemsteuerung** auf **Windows Firewall**.
2. Klicken Sie auf der Registerkarte **Allgemein** auf **Aus** und anschließend auf **OK**.

So aktivieren und konfigurieren Sie Windows Firewall auf einem Dateiserver

1. Klicken Sie in der **Systemsteuerung** auf **Windows Firewall**.
2. Klicken Sie auf der Registerkarte **Allgemein** auf **Ein**, und überprüfen Sie, ob das Kontrollkästchen **Keine Ausnahmen zulassen** deaktiviert ist.
3. Führen Sie auf der Registerkarte **Ausnahmen** folgende Aufgaben durch:
   - Klicken Sie auf **Programm hinzufügen**, dann auf **Durchsuchen**, und wechseln Sie in das Verzeichnis **Programme/Microsoft Data Protection Manager/DPM/bin**. Wählen Sie **Msdpmfsagentca.exe** aus, klicken Sie auf **Öffnen** und anschließend auf **OK**.
   - Klicken Sie auf **Anschluss hinzufügen**, geben Sie im Feld **Name** einen Namen für den Port ein (jeder Name ist zulässig), geben Sie im Feld **Portnummer** den Wert **135** ein, überprüfen Sie, ob **TCP** als Protokoll festgelegt ist, klicken Sie auf **OK**, um das Dialogfeld **Anschluss hinzufügen** zu schließen und erneut auf **OK**, um das Dialogfeld **Windows Firewall** zu schließen.

KAPITEL 5

Archivieren und Wiederherstellen von Daten

Nach dem Bereitstellen von Microsoft System Center Data Protection Manager (DPM) können Sie mit DPM und dessen Funktionen für die Wiederherstellung von auf Festplatten gespeicherten Daten den Großteil der erforderlichen kurzfristigen Datenwiederherstellungsanforderungen erfüllen. Zusätzlich können Sie für die langfristige Datenarchivierung und Datenwiederherstellung im Notfall weiterhin Sicherheitskopien auf Band verwenden. DPM lässt sich problemlos in bestehende Archivierungslösungen integrieren.

Indem Dateiserverdaten nicht direkt vom Dateiserver, sondern von den Replikaten auf dem DPM-Server archiviert werden, kann das Erstellen von Sicherungskopien unabhängig von der Verfügbarkeit des Dateiservers geplant werden. Wenn Sie die DPM-Serverdaten auf Band sichern, können Sie im Notfall archivierte Daten auf den Dateiservern wiederherstellen und den DPM-Server neu erstellen.

In diesem Kapitel wird das Planen und Bereitstellen einer Lösung zum Archivieren von Datendateien und Erstellen einer DPM-Sicherungskopie auf Band erläutert. Es werden allgemein die Vorgänge des Archivierens und Wiederherstellens von DPM mithilfe verschiedener Arten von Sicherungssoftware beschrieben. Die genauen Vorgänge unterscheiden sich zwischen den unterschiedlichen Sicherungssoftwareprodukten.

Hinweis

Eine Anleitung für das Wiederherstellen von Daten mit DPM finden Sie im Abschnitt „Recovering Data“ (http://go.microsoft.com/fwlink/?LinkId=51984, in englischer Sprache) in der DPM-Hilfe. Informationen zur Problembehandlung bei der Datenwiederherstellung mit DPM finden Sie im Kapitel „Problembehandlung“ (http://go.microsoft.com/fwlink/?LinkId=46369) in diesem Handbuch.

In diesem Kapitel

Planen der Archivierung und Wiederherstellung von Daten

- Ermitteln der Sicherungskomponenten
- Planen von Sicherungen
- Auswählen von Sicherungssoftware
  - Sicherungssoftware, die DPM unterstützt
  - Sicherungssoftware, die VSS unterstützt
  - Sicherungssoftware, die VSS nicht unterstützt
- Integrieren von DPM in eine Sicherungstopologie

Sichern von Servern

Archivieren von Datenbanken und Replikaten

- Verwenden von Sicherungssoftware, die DPM unterstützt
- Verwenden von Sicherungssoftware, die VSS unterstützt

Verwenden von Sicherungssoftware, die VSS nicht unterstützt
Verwenden von DpmBackup zum Erstellen von Sicherungsschattenkopien
DpmBackup-Syntax
Verwenden von DpmBackup mit Bereitstellungspunkten
Wiederherstellen von Daten vom Band auf Dateiserver
Verwenden von FsPathMerge zum Reparieren von Pfaden auf Dateiservern
FsPathMerge-Syntax
Wiederherstellen eines DPM-Servers
Wiederherstellen von Datenbanken
Verwenden von DpmSync zum Wiederherstellen von Datenbanken
DpmSync-Syntax
Wiederherstellen von Replikaten
Verwenden von DpmPathMerge zum Reparieren von Pfaden
DpmPathMerge-Syntax
Verwenden von FsPathMerge zum Reparieren von Pfaden auf einem DPM-Server
Wiederherstellen eines DPM-Servers auf einem neuen Computer

Planen der Archivierung und Wiederherstellung von Daten

DPM bietet eine hervorragende Lösung für kurzfristigen Schutz und das Wiederherstellen von Dateiserverdaten. Allerdings bleibt die Notwendigkeit, Dateiserverdaten für die langfristige Speicherung und das Wiederherstellen in Notfällen zu archivieren, weiterhin bestehen. Die Hauptgründe, Dateiserverdaten auch nach dem Bereitstellen von DPM zu archivieren sind geschäftliche, rechtliche oder finanzielle Anforderungen an die Datenarchivierung, sowie die Möglichkeit einer vollständigen Wiederherstellung bei Hardware- oder Softwarenotfällen auf dem DPM-Server sowie bei einem Sitenotfall, der sowohl den DPM-Server als auch die geschützten Dateiserver betrifft.

Beim Entwerfen der Archivierungsstrategie sollten Sie verschiedene Überlegungen berücksichtigen, z. B. das Wiederherstellen ausschließlich notwendiger Daten, das sorgfältige Planen von Sicherungsvorgängen und das Auswählen geeigneter Tools zum Sichern und Wiederherstellen von Daten. Die Archivierungs- und Wiederherstellungsstrategie sollte mindestens folgende Faktoren einschließen:

• Eine Liste der Sicherungskomponenten

• Einen Zeitplan für die Sicherung

• Sicherungssoftware und -tools

• Eine Sicherungstopologie

Hinweis

Weitere Informationen zum Entwerfen einer Wiederherstellungsstrategie für Notfälle in Windows 2000 Server- und Windows Server 2003-Umgebungen finden Sie im Microsoft TechNet-Artikel „Planning for Disaster Recovery“ (http://go.microsoft.com/fwlink/?LinkId=47882, in englischer Sprache).

In den folgenden Abschnitten finden Sie ausführlichere Informationen über das Planen einer Archivierungs- und Wiederherstellungsstrategie in der DPM-Umgebung.

Ermitteln der Sicherungskomponenten

Sie müssen alle Komponenten ermitteln, die gesichert werden müssen, um die Anforderungen für die Datenarchivierung und Notfall-Wiederherstellung zu erfüllen. Mithilfe von DPM können Sie durch Archivieren des DPM-Servers sowohl die Anforderungen an die Archivierung als auch die Wiederherstellung in Notfällen erfüllen. Da auf dem DPM-Server Replikate der Dateiserverdaten gespeichert sind, archivieren Sie bei Archivierung des DPM-Servers gleichzeitig die Daten der Dateiserver. Um eine vollständige Wiederherstellung des DPM-Servers zu ermöglichen, müssen folgende Komponenten auf Band gesichert werden:

- Systemstatus
- Programmdateien
- Datenbanken
    - Die DPM-Datenbank (DPMDB.mdf)
    - Die Berichtsdatenbank (ReportServer.mdf)
- Replikate

Das Sichern der Replikate vom DPM-Server bietet gegenüber dem Sichern der Dateien von den einzelnen Dateiservern zwei entscheidende Vorteile. Erstens wird das Erstellen und Verwalten von Archiven vereinfacht, da Daten verschiedener Dateiserver von einem einzigen Ort archiviert werden können, dem DPM-Server. Zweitens wirkt sich der Sicherungsprozess nicht auf die aktiven Vorgänge aus, die Serverressourcen erfordern, da die Replikate als Quelle für die Sicherung verwendet werden.

Planen von Sicherungen

Legen Sie fest, wann manuelle Sicherungen und wie oft regelmäßige Sicherungen ausgeführt werden müssen. Sofern Geschäftsanforderungen nicht eine andere Vorgehensweise erfordern, wird empfohlen, die Datenbanken und Replikate nach dem erstmaligen Erstellen, nach Hinzufügen neuer Schutzgruppen oder nach vorgenommenen Änderungen an Schutzgruppen zu sichern und danach wöchentliche Sicherungen durchzuführen.

Beachten Sie beim Erstellen eines Sicherungsplans die geschäftlichen, rechtlichen und behördlichen Anforderungen an das Archivieren von Dateiserverdaten. Die Häufigkeit der Sicherungen und die Aufbewahrungsdauer der Daten können durch behördliche und geschäftliche Anforderungen festgelegt werden. Da DPM für das kurzfristige Wiederherstellen von Daten verwendet wird, sollte der Plan für Bandsicherungen auf Grundlage der Anforderungen an die langfristige Datenspeicherung erstellt werden.

Auswählen von Sicherungssoftware

DPM-Replikate und -Datenbanken lassen sich am besten mithilfe von Sicherungssoftware archivieren, die speziell für die Verwendung mit DPM entworfen wurde. Sie können die Replikate und Datenbanken jedoch auch mit Sicherungssoftware archivieren, die DPM nicht unterstützt. Wenn Sie Software verwenden, die DPM nicht unterstützt, unterscheidet sich der Archivierungsvorgang für Replikate und Datenbanken, je nachdem ob die Sicherungssoftware den Volumeschattenkopie-Dienst (VSS – Volume Shadow Copy Service) unterstützt.

Die Sicherungssoftware lässt sich in drei Typen einteilen, die in Tabelle 5.1 aufgeführt sind.

Tabelle 5.1 Sicherungssoftwaretypen

Typ	Unterstützt DPM	Unterstützt VSS (Volume Shadow Copy Service)
DPM-kompatibel	Ja	Ja
VSS-kompatibel	Nein	Ja
Nicht VSS-kompatibel	Nein	Nein

Sicherungssoftware, die DPM unterstützt

Wenn Sie die Möglichkeit haben, neue Sicherungssoftware zu installieren, wird das Verwenden von Sicherungssoftware empfohlen, die speziell für das Zusammenarbeiten mit DPM entworfen wurde. Diese Software unterstützt VSS und den DPM VSS Writer-Dienst (DPM Writer).

DPM Writer ist ein Service, der zum Zweck der Datenarchivierung Sicherungsschattenkopien von DPM-Replikaten und Schattenkopien des Volumes verwaltet, das die DPM- und Berichtdatenbanken enthält. Der DPM Writer-Dienst wird vom Befehlszeilentool DpmBackup oder einem DPM-kompatiblen VSS-Anforderer verwendet. DPM Writer implementiert einen VSS Writer für DPM. VSS-Anforderer können Volumes mit dem DPM VSS Writer, die von DPM geschützt werden, sichern und wiederherstellen. Anforderer können mithilfe des DPM Writer außerdem DPM- und Berichtdatenbanken sichern.

Sicherungssoftware, die DPM unterstützt, bietet zwei entscheidende Vorteile:

- Die Anzahl notwendiger Arbeitsschritte für Archivierungs- und Wiederherstellungsvorgänge wird minimiert.
- Die archivierten Replikate werden so organisiert, dass sie wie direkt von den geschützten Dateiservern gesicherte Replikate angezeigt werden. Durch diese Art der Organisation wird der Datenwiederherstellungsprozess intuitiver.

Informationen über spezifische Software, die für die Zusammenarbeit mit DPM entworfen wurde, finden Sie im Abschnitt „Technical Resources“ auf der DPM Web site (http://go.microsoft.com/fwlink?linkid=33686, in englischer Sprache).

Sicherungssoftware, die VSS unterstützt

Sicherungssoftware, die VSS unterstützt, verwendet VSS-kompatible Dateisystemschattenkopien, arbeitet jedoch nicht mit dem DPM Writer-Dienst. Diese Software hat zwei Nachteile verglichen mit Software, die DPM unterstützt. Zum einen sind Archivierungs- und Wiederherstellungsvorgänge komplexer als mit Software, die DPM unterstützt. Zum anderen organisiert Software, die VSS unterstützt, die archivierten Replikate so, dass sie als direkt vom DPM-Server gesichert angezeigt werden. Durch diese Art der Organisation wird der Datenwiederherstellungsprozess weniger intuitiv.

Informationen über das Verwenden von DPM mit Software, die VSS unterstützt, finden Sie im Abschnitt „Technical Resources“ auf der DPM Web site (http://go.microsoft.com/fwlink?linkid=33686, in englischer Sprache).

Sicherungssoftware, die VSS nicht unterstützt

Wenn Sie Sicherungssoftware verwenden, die VSS nicht unterstützt, können Sie nicht direkt von den Replikaten sichern. Stattdessen müssen Sie mit dem Tool DpmBackup Sicherungsschattenkopien von den Replikaten und Datenbanksicherungskopien von den DPM- und Berichtdatenbanken erstellen und anschließend mit der Sicherungssoftware die Sicherungsschattenkopien und Datenbanksicherungskopien auf Band sichern.

Weitere Informationen zu DpmBackup finden Sie im Abschnitt „Verwenden von Sicherungssoftware, die VSS nicht unterstützt“ in diesem Kapitel.

Sicherungstools in DPM

DPM beinhaltet mehrere Befehlszeilentools zum Sichern und Wiederherstellen von DPM-Daten. Welche DPM-Tools Sie verwenden ist von der Art der verwendeten Sicherungssoftware abhängig.

In Tabelle 5.2 finden Sie eine Übersicht, welche DPM-Befehlszeilentools mit den verschiedenen Sicherungssoftwaretypen verwendet werden können.

Tabelle 5.2 Sicherungssoftware und DPM-Sicherungstools

Sicherungssoftwaretyp	Zu verwendendes DPM-Sicherungstool
Sicherungssoftware, die DPM unterstützt	DpmSync zum Wiederherstellen und Synchronisieren von Datenbanken sowie zum erneuten Zuweisen von Replikaten.
Sicherungssoftware, die VSS unterstützt	DpmSync zum Wiederherstellen und Synchronisieren von Datenbanken sowie zum erneuten Zuweisen von Replikaten (siehe „Verwenden von DpmSync zum Wiederherstellen von Datenbanken“). FsPathMerge zum Löschen überflüssiger Pfadinformationen aus sämtlichen wiederhergestellten Replikaten (siehe „Verwenden von FsPathMerge zum Reparieren von Pfaden auf Dateiservern“).

Sicherungssoftware, die VSS nicht unterstützt	DpmBackup zum Vorbereiten der Dateien und Datenbanken für die Sicherung (siehe „Verwenden von DpmBackup zum Erstellen von Sicherungsschattenkopien“). DpmSync zum Wiederherstellen und Synchronisieren von Datenbanken sowie zum erneuten Zuweisen von Replikaten (siehe „Verwenden von DpmSync zum Wiederherstellen von Datenbanken“). FsPathMerge zum Löschen überflüssiger Pfadinformationen aus sämtlichen wiederhergestellten Replikaten (siehe „Verwenden von FsPathMerge zum Reparieren von Pfaden auf Dateiservern“). DpmPathMerge zum Löschen überflüssiger Pfadinformationen aus sämtlichen wiederhergestellten Replikaten (siehe „Verwenden von DpmPathMerge zum Reparieren von Pfaden“).

Integrieren von DPM in eine Sicherungstopologie

Sicherungstopologien variieren von lokalen Speichergeräten, die mit einzelnen Servern verbunden sind, bis hin zu SAN-(Storage Area Network-)Lösungen. DPM bietet unabhängig von der im Netzwerk verwendeten Topologie zwei Vorteile:

- Da die kurzfristige Sicherung von Datendateien vom DPM-Server durchgeführt wird, reduzieren sich die Netzwerklast für Sicherungen und die Bandanforderungen.
- Da die Anforderungen für die Dateiarchivierung durch Sichern des DPM-Servers anstelle der einzelnen Dateiserver erfüllt werden können, sind weniger Sicherungsagentlizenzen erforderlich.

Weitere Informationen zum Planen einer Lösung zur Notfall-Wiederherstellung, die DPM mit einschließt, finden Sie im Microsoft System Center Data Protection Manager 2006 Planungs- und Bereitstellungshandbuch (http://go.microsoft.com/fwlink/?LinkId=46351, in englischer Sprache).

Beispielcode für das Sichern und Wiederherstellen eines DPM-Servers und für das Wiederherstellen eines Dateiservers erhalten Sie, wenn Sie das Volume Shadow Copy Services Writer Software Development Kit (VSS SDK) 1.0 für DPM per E-Mail unter dpspart@microsoft.com (in englischer Sprache) anfordern. Das SDK wird auch als Download im Microsoft Storage Partner Extranet zur Verfügung stehen (http://go.microsoft.com/fwlink/?LinkId=45789; in englischer Sprache). Sie müssen sich auf dieser Site registrieren, damit Sie Software herunterladen können.

Sichern von Servern

Um eine vollständige Wiederherstellung eines DPM- oder Dateiservers durchführen zu können, müssen Sie zuvor das Betriebssystem, die Anwendungen und die Serverkonfiguration sichern. Eine Methode zum Archivieren des Systemstatus ist das Verwenden von Backup, der Sicherungssoftware in Windows Server 2003.

Mithilfe von Backup können Sie einen automatischen Systemwiederherstellungssatz (ASR – Automated System Recovery) erstellen. Der ASR-Satz beinhaltet eine Sicherung des Systemstatus, der Systemdienste und sämtlicher Datenträger, die den Betriebssystemkomponenten zugeordnet sind. Im Satz ist außerdem ein Startdatenträger mit Informationen über die Sicherungskopie und die Festplattenkonfigurationen enthalten. Erstellen Sie regelmäßig und vor allem nach umfassenden Systemänderungen einen neuen automatischen Systemwiederherstellungssatz.

Mit Backup können Sie außerdem den Systemstatus in eine Datei exportieren, sodass Sie den Systemstatus sichern können, ohne einen ASR-Satz erstellen zu müssen. Backup sollte so konfiguriert werden, dass der Systemstatus für eine Archivierung auf Band regelmäßig in eine Datei exportiert wird.

Weitere Informationen zum Verwenden von Backup zum Archivieren des Systemstatus finden Sie im Whitepaper „Using Data Protection Manager with Windows Backup“ unter „Technical Resources“ auf der DPM Web site (http://go.microsoft.com/fwlink?linkid=33686, in englischer Sprache). Weitere Informationen zu Backup und ASR finden Sie im Artikel „Safeguarding your system“ (in englischer Sprache) oder suchen Sie nach dem Begriff „Backup“ im Support Center von Windows Server 2003.

Warnung

Es ist wichtig, dass Sie die DPM-Servervolumes sichern, auf denen die Systemdateien für DPM, SQL Server und SQL Server Reporting Services enthalten sind. Nach einem Notfall, bei dem nur einige der von DPM benötigten Dateien verloren gegangen sind, können Sie DPM erst installieren oder deinstallieren, nachdem Sie die Volumes mit den benötigten Dateien wiederhergestellt haben.

Archivieren von Datenbanken und Replikaten

Die DPM-Datenbanken und die Replikate sind die für den DPM-Server notwendigen Komponenten, die für die langfristige Speicherung und die Notfall-Wiederherstellung gesichert werden müssen. Der Sicherungsvorgang für die DPM-Datenbanken und Replikate ist von der von Ihnen verwendeten Sicherungssoftware abhängig. Anleitungen zum Verwenden der folgenden Sicherungssoftwaretypen finden Sie in diesen Abschnitten:

- Sicherungssoftware, die DPM unterstützt
- Sicherungssoftware, die VSS unterstützt
- Sicherungssoftware, die weder DPM noch VSS unterstützt

Verwenden von Sicherungssoftware, die DPM unterstützt

DPM-Replikate und -Datenbanken lassen sich am besten mithilfe von Sicherungssoftware archivieren, die speziell für die Verwendung mit DPM entworfen wurde. Die Hauptvorteile von Software, die DPM unterstützt, liegen darin, dass archivierte Daten so organisiert werden, dass Wiederherstellungsvorgänge intuitiv und relativ einfach durchgeführt werden können, und dass die Anzahl der für das Archivieren und Wiederherstellen notwendigen Schritte minimiert wird.

Sie müssen die Datenbank- und Transaktionsprotokolldateien sowohl für die DPM- als auch für die Berichtdatenbank sichern. (Durch das Sichern der Datenbanken werden die zugehörigen Transaktionsprotokolldateien automatisch gesichert.) Im Folgenden finden Sie allgemeine Anleitungen zum Archivieren von DPM-Datenbanken und Replikaten mithilfe von Sicherungssoftware, die DPM unterstützt. Eine Anleitung für das Verwenden der Sicherungssoftware finden Sie in der Dokumentation der Sicherungssoftware.

So sichern Sie Datenbanken mithilfe von DPM-kompatibler Sicherungssoftware

1. Wechseln Sie in der Konsolenstruktur des Sicherungsprogramms in das Verzeichnis **\Programme\Microsoft Data Protection Manager\DPM**, und wählen Sie den Ordner **DPMDB** aus. Der Dateiname der DPM-Datenbankdatei ist DPMDB2006.mdf. Der Dateiname der Transaktionsprotokolldatei für diese Datenbank ist DPMDB_log2006.ldf.
2. Wechseln Sie in der Konsolenstruktur des Sicherungsprogramms in das Verzeichnis **\Programme\Microsoft Data Protection Manager\Prerequisites\MSSQL$MICROSOFT$DPM$**, und wählen Sie den Ordner **Data** aus. Der Name der Berichtsdatenbankdatei lautet in der Standardeinstellung ReportServer.mdf. Der Name der Transaktionsprotokolldatei für diese Datenbank lautet in der Standardeinstellung ReportServer_log.ldf.
3. Wählen Sie das Medium aus, auf welches die Datenbanken gesichert werden sollen.
4. Starten Sie den Sicherungsvorgang.

Sicherungssoftware, die DPM unterstützt, interagiert mit dem DPM Writer-Dienst und VSS, um eine Schattenkopie des Replikats und anschließend eine Sicherungskopie der Schattenkopie zu erstellen.

So sichern Sie Replikate mithilfe von DPM-kompatibler Sicherungssoftware

1. Erweitern Sie in der Konsolenstruktur des Sicherungsprogramms den Knoten für den DPM-Server.
2. Wählen Sie den Dateiserver aus, dessen Replikate Sie archivieren möchten, oder die einzelnen geschützten Volumes.
3. Wählen Sie den Sicherungstyp aus.
4. Wählen Sie das Medium aus, auf das die Dateien gesichert werden sollen.
5. Starten Sie den Sicherungsvorgang.

Verwenden von Sicherungssoftware, die VSS unterstützt

Wenn die Sicherungssoftware VSS unterstützt, können Sie Daten direkt von den Replikaten unter **Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica** sichern. Allerdings müssen Sie sicherstellen, dass die Software keine Daten auf den Replikatvolumes ändert. Lesen Sie die Dokumentation der Sicherungssoftware, oder wenden Sie sich an den Hersteller, um die Sicherungsarten für diese Software zu ermitteln, bei der keine Daten auf den Replikatvolumes geändert werden. Wenn Sie z. B. das Windows-Sicherungsprogramm zum Archivieren von Daten verwenden, können Sie nur die Sicherungsart „Kopieren“ verwenden.

Sie müssen die Datenbank- und Transaktionsprotokolldateien sowohl für die DPM- als auch für die Berichtdatenbank sichern. Im Folgenden finden Sie allgemeine Anleitungen zum Archivieren von DPM-Datenbanken und Replikaten mithilfe von Sicherungssoftware, die zwar nicht DPM, jedoch VSS unterstützt. Eine Anleitung für das Verwenden der Sicherungssoftware finden Sie in der Dokumentation der Sicherungssoftware.

So sichern Sie Datenbanken mithilfe von Sicherungssoftware, die VSS unterstützt

1. Wechseln Sie in der Konsolenstruktur des Sicherungsprogramms in das Verzeichnis **\Programme\Microsoft Data Protection Manager\DPM**, und wählen Sie den Ordner **DPMDB** aus. Der Dateiname der DPM-Datenbankdatei ist DPMDB2006.mdf. Der Dateiname der Transaktionsprotokolldatei für diese Datenbank ist DPMDB_log2006.ldf.
2. Wechseln Sie in der Konsolenstruktur des Sicherungsprogramms in das Verzeichnis **\Programme\Microsoft Data Protection Manager\Prerequisites\MSSQL$MICROSOFT$DPM$**, und wählen Sie den Ordner **Data** aus. Der Name der Berichtsdatenbankdatei lautet in der Standardeinstellung ReportServer.mdf. Der Name der Transaktionsprotokolldatei für diese Datenbank lautet in der Standardeinstellung ReportServer_log.ldf.
3. Wählen Sie das Medium aus, auf das die Datenbanken gesichert werden sollen.
4. Starten Sie den Sicherungsvorgang.

Hinweis

Einige VSS-kompatible Sicherungssoftwareprodukte verfügen nicht über einen SQL VSS-Anforderer für das Sichern von SQL Server-Datenbanken mithilfe der VSS-Infrastruktur und des MSDE VSS Writer. Verwenden Sie in diesem Fall die Methode zum Sichern von Datenbanken mit nicht VSS-kompatibler Sicherungssoftware.

So sichern Sie Replikate mithilfe von VSS-kompatibler Sicherungssoftware

1. Wechseln Sie in der Konsolenstruktur des Sicherungsprogramms in das Verzeichnis **\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica** auf dem DPM-Server.
2. Wählen Sie den Dateiserver aus, dessen Replikate Sie archivieren möchten, oder die einzelnen geschützten Volumes.
3. Wählen Sie den Sicherungstyp aus.

   Wichtig

   Lesen Sie die Dokumentation der Sicherungssoftware, oder wenden Sie sich an den Hersteller, um die Sicherungsarten zu ermitteln, bei denen Replikatdaten nicht geändert werden.
4. Wählen Sie das Medium aus, auf das die Dateien gesichert werden sollen.
5. Starten Sie den Sicherungsvorgang.

Verwenden von Sicherungssoftware, die VSS nicht unterstützt

Wenn die Sicherungssoftware VSS oder DPM nicht unterstützt, müssen Sie mit dem Befehlszeilentool DpmBackup Sicherungsschattenkopien von den Replikaten und Datenbanksicherungskopien von den DPM- und Berichtdatenbanken erstellen und anschließend mit der Sicherungssoftware die Sicherungsschattenkopien und Datenbanksicherungskopien auf Band sichern.

Folgende Themen werden in diesem Abschnitt behandelt:

• Verwenden von DpmBackup zum Erstellen von Sicherungsschattenkopien

• DpmBackup-Syntax

• Verwenden von DpmBackup mit Bereitstellungspunkten

Verwenden von DpmBackup zum Erstellen von Sicherungsschattenkopien

Mit DpmBackup können Sie Dateien für die Sicherung vorbereiten, wenn Sie Sicherungssoftware verwenden, die nicht VSS-kompatibel ist. DpmBackup ist ein in DPM enthaltenes Befehlszeilenprogramm zum Ausführen folgender Aufgaben:

- Erstellen und Bereitstellen von Sicherungsschattenkopien sämtlicher Replikatvolumes auf dem DPM-Server.
- Erstellen von Datenbanksicherungskopien der DPM-Datenbank (DPMDB.mdf) und der Berichtdatenbank (ReportServer.mdf).

DPM erstellt einen Bereitstellungspunkt der Sicherungsschattenkopien der Replikate auf dem DPM-Server im Ordner **Programme\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy**. Die Sicherungsschattenkopien der Replikate werden nach Dateiservern organisiert.

Sie können entweder das Bandsicherungsprogramm oder den Windows-Planer so konfigurieren, dass DpmBackup ausgeführt wird, bevor das Bandsicherungsprogramm ausgeführt wird. Wie viel Zeit DpmBackup zum Erstellen der Sicherungsschattenkopien und Datenbanksicherungskopien benötigt, ist von Faktoren wie Festplatten- und Datenbankaktivität abhängig. In der Regel benötigt das Tool zum Abschließen des Vorgangs jedoch ungefähr zwei Minuten pro Replikatvolume.

Das Programm DpmBackup.exe ist auf dem DPM-Server im Ordner **Programme\Microsoft Data Protection Manager\DPM\bin** gespeichert. DpmBackup benötigt Administrator- oder Sicherungs-Operator-Zugriffsrechte für den DPM-Server.

Die von DpmBackup erstellten Sicherungsschattenkopien sind schreibgeschützte Kopien der Replikatvolumes und können wie ein gewöhnliches Dateisystem archiviert werden. Da die Sicherungsschattenkopien der Replikate über Bereitstellungspunkte bereitgestellt werden, muss die Bandsicherungssoftware so konfiguriert werden, dass sie mit Bereitstellungspunkten umgehen kann.

Informationen zur Problembehandlung für DpmBackup finden Sie im Kapitel „Problembehandlung“ in diesem Handbuch (http://go.microsoft.com/fwlink/?LinkId=46369).

Sie müssen die Datenbank- und Transaktionsprotokolldateien sowohl für die DPM- als auch für die Berichtdatenbank sichern. Im Folgenden finden Sie allgemeine Anleitungen zum Archivieren von DPM-Datenbanken und Replikaten mithilfe von Sicherungssoftware, die weder DPM noch VSS unterstützt. Eine Anleitung für das Verwenden der Sicherungssoftware finden Sie in der Dokumentation der Sicherungssoftware.

So sichern Sie Datenbanken mithilfe von Sicherungssoftware, die weder DPM noch VSS unterstützt

1. Führen Sie das Tool DpmBackup aus.

   Sie können das Tool manuell ausführen oder das Sicherungsprogramm so konfigurieren, dass es automatisch ausgeführt wird.

2. Wechseln Sie in der Konsolenstruktur des Sicherungsprogramms in das Verzeichnis **\Programme\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy\Database Backups**. Der Dateiname der Sicherungskopie der DPM-Datenbank ist DPMDB.bak. Der Dateiname der Sicherungskopie der Berichtdatenbank ist in der Standardeinstellung ReportServer.bak.
3. Wählen Sie das Medium aus, auf das die Datenbanken gesichert werden sollen.
4. Starten Sie den Sicherungsvorgang.

So sichern Sie Replikate mithilfe von Sicherungssoftware, die weder DPM noch VSS unterstützt

1. Führen Sie das Tool DpmBackup aus. Sie können das Tool manuell ausführen oder das Sicherungsprogramm so konfigurieren, dass es automatisch ausgeführt wird.
2. Wechseln Sie in der Konsolenstruktur des Sicherungsprogramms in das Verzeichnis **\Programme\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy**. Die Sicherungsschattenkopien der Replikate werden nach Dateiservern organisiert.
3. Wählen Sie die zu sichernden Schattenkopien aus.
4. Wählen Sie den Sicherungstyp aus.
5. Wählen Sie das Medium aus, auf das die Dateien gesichert werden sollen.
6. Starten Sie den Sicherungsvorgang.

DpmBackup-Syntax

DpmBackup

DpmBackup -?

Parameter

Parameter	Beschreibung
Keine Argumente	Es werden Sicherungsschattenkopien der DPM-Replikate und Sicherungskopien der DPM- und Berichtdatenbanken im Ordner **Programme\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy\Database Backups** erstellt, die nach Dateiservern organisiert werden.
-?	Beschreibt die Verwendung des Befehls.

Verwenden von DpmBackup mit Bereitstellungspunkten

Wenn Sie DpmBackup ausführen und Volumes ohne zugewiesene Laufwerksbuchstaben (Volumebereitstellungspunkte) schützen, werden die von DpmBackup erstellten Sicherungsschattenkopien nur mit der GUID im DPM-Namespace bereitgestellt. Verwenden Sie das Dokument **DpmMetadata.xml**, um die Zuordnung zwischen der Volume-GUID im geschützten Pfad auf dem DPM-Server und dem tatsächlichen geschützten Volume auf dem geschützten Dateiserver zu erkennen. Das Dokument wird erstellt, wenn Sie DpmBackup erfolgreich ausführen.

DpmMetadata.xml wird im Ordner **\Programme\Microsoft Data Protection Manager\DPM\Backup Documents** gespeichert. **DpmMetadata.xml** bietet eine XML-Ansicht der DPM-Topologie, wie in folgendem Beispiel dargestellt.

Beispiel

Volumebereitstellungspunkt auf dem geschützten Dateiserver FS01 (Volume-GUID: 7fa3a5e6-929c-11d9-a3b7-000c76289bfb)	**C:\mountpoints\volume6**
Von DpmBackup erstellter Pfad	**C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Shadowcopy\FS01\7fa3a5e6-929c-11d9-a3b7-000c76289bfb\Replicadir**
Geschützter Pfad auf dem DPM-Server	**C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\7fa3a5e6-929c-11d9-a3b7-000c76289bfb\Replicadir**

Darstellung in **DpmMetadata.xml**	`<Component Name="Replica\Mount point C:\mountpoints\volume6 on server FS01">`
	`<RestoreData ProtectionGroup="Sales" FileServer="FS01"`
	`FileServerVolumeGUID="\\?\Volume{7fa3a5e6-929c-11d9-a3b7-000c76289bfb}\"`
	`FileServerBasePath="C:\mountpoints\volume6\"`
	`DpmServerBasePath="C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\`
	`7fa3a5e6-929c-11d9-a3b7-000c76289bfb\ReplicaDir\" />`
	`</Component>`

Wiederherstellen von Daten vom Band auf Dateiserver

In den meisten Fällen können Sie Daten für einen Dateiserver mithilfe der Wiederherstellungsfunktionen der DPM-Verwaltungskonsole wiederherstellen. Endbenutzer verwenden zur Wiederherstellung von Dateien die Endbenutzerwiederherstellung. Sie können jedoch auch Daten aus einem Bandarchiv für einen Dateiserver wiederherstellen, wenn Sie z. B. eine ältere Version als die in den bestehenden Replikaten wiederherstellen möchten, oder wenn sowohl der Dateiserver als auch der DPM-Server ausfallen. Informationen bezüglich der Wiederherstellung von Daten auf Band für Dateiserver finden Sie in der Dokumentation zur Sicherungsanwendung.

Die meisten Sicherungsprogramme hängen den Originalpfad der Datei an den angegebenen Zielordner an. Sicherungssoftware, die DPM unterstützt, stellt Dateien in den festgelegten Zielordnern wieder her, ohne den Originalpfad anzuhängen. Wenn Sie Sicherungssoftware verwenden, die DPM nicht unterstützt, müssen Sie nach Wiederherstellen der Replikatsicherung im geschützten Ordner des Dateiservers die Pfadnamen reparieren, indem Sie FsPathMerge auf dem Dateiserver ausführen.

Wichtig

Aus Sicherheitsgründen bezieht DPM in Replikaten oder Schattenkopien geschützter Daten keine Analysepunkte mit ein. Nachdem Sie ein Volume, einen Ordner oder eine Freigabe mit einem Analysepunkt wiederhergestellt haben, müssen Sie den Analysepunkt manuell neu erstellen. (Sie können jedoch das Ziel eines Analysepunkts genau wie alle anderen geschützten Volumes, Ordner oder Freigaben wieder herstellen, wenn das Ziel Mitglied einer Schutzgruppe ist.)

Eine Anleitung zum Wiederherstellen des Schutzes auf einem Dateiserver nach einem Laufwerkfehler oder einer Datenträgeraktualisierung finden Sie in diesem Handbuch im Kapitel „Verwalten von Servern“ (http://go.microsoft.com/fwlink/?LinkId=46367)

Verwenden von FsPathMerge zum Reparieren von Pfaden auf Dateiservern

FsPathMerge ist ein in DPM enthaltenes Befehlszeilenprogramm, das überflüssige Pfadinformationen von Daten löscht, die auf einem geschützten Dateiserver wiederhergestellt wurden. Nachdem sämtliche Dateiserverdaten wiederhergestellt wurden, führen Sie FsPathMerge für alle Replikate auf dem Dateiserver aus. Das Programm FsPathMerge.exe befindet sich auf der DPM-Installations-CD im Ordner **Support\Tools**.

Hinweis

Lokalisierte Versionen von FsPathMerge.exe befinden sich unter **Support\Tools** im der jeweiligen Sprache entsprechenden Ordner.

FsPathMerge benötigt Administrator- oder Sicherungs-Operator-Zugriffsrechte für den Dateiserver. In FsPathMerge können nur vollqualifizierte Pfade verwendet werden. Verwenden Sie kein UNC-Format. Der wiederhergestellte Pfad und der Zielpfad müssen sich auf demselben Laufwerk befinden. Windows-Tools können keine Pfade anzeigen, die mehr als 256 Zeichen enthalten. Verwenden Sie daher die von der Sicherungssoftware erstellten Sicherungsprotokolle, um die Pfadinformationen zu ermitteln, wenn Sie FsPathMerge verwenden, um Daten aus den Replikaten wiederherzustellen.

Wichtig

Stellen Sie sicher, dass keine Anwendungen auf die wiederhergestellten Dateien zugreifen, bevor Sie FsPathMerge ausführen. Wenn der Befehl die Meldung „Zugriff verweigert“ zurückgibt, bedeutet das, dass eine Anwendung eine der Dateien verwendet, die FsPathMerge verschieben möchte.

Informationen zur Problembehandlung für FsPathMerge finden Sie im Kapitel „Problembehandlung“ in diesem Handbuch (http://go.microsoft.com/fwlink/?LinkId=46369).

FsPathMerge-Syntax

FsPathMerge **–FS** *WiederhergestellterPad ZielPfad*

FsPathMerge **–FS** *WiederhergestellterPad ZielPfad* **-Y**

FsPathMerge **–D** *ZielPfad*

FsPathMerge **-?**

Parameter

Parameter	Beschreibung
WiederhergestellterPfad	Der Pfad, in dem die Sicherungssoftware die Daten wiederhergestellt hat.
ZielPfad	Der Pfad, in dem die Daten wiederhergestellt werden sollen.
-FS	Führt die Inhalte aus *WiederhergestellterPfad* mit dem *ZielPfad* zusammen, nachdem Daten von Band auf einem Dateiserver wiederhergestellt wurden.
-Y	Löscht bei der Zusammenführung die ursprünglichen Inhalte des Zielpfades. (Vorsicht: Vorhandene Daten im Zielpfad werden mit dieser Option gelöscht.)
-D	Löscht den Inhalt des Zielpfades in einem separaten Vorgang.
-?	Beschreibt die Verwendung des Befehls.

Beispiel

Sie schützen den Ordner **C:\Sales** auf dem Dateiserver **FS01**. Führen Sie DpmBackup auf dem DPM-Server aus, um das Replikat für die Sicherung vorzubereiten. Die Sicherungsschattenkopie von **C:\Sales** befindet sich unter **C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy\FS01\C-8d2a01f3-4b01-11d9-b735-806e6f6e6963\ReplicaDir\Sales**.

Die Sicherungsschattenkopie auf dem DPM-Server wird auf Band gesichert. Wenn Sie den Ordner **Sales** von Band für den Dateiserver **FS01** wiederherstellen, wird folgender Pfad erstellt:

C:\Sales\Programme\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy\FS01\C-8d2a01f3-4b01-11d9-b735-806e6f6e6963\Replicadir\Sales

Führen Sie folgenden Befehl aus, um die richtigen Pfadinformationen wiederherzustellen.

```
FsPathMerge.exe –FS „C:\Sales\Programme\Microsoft Data Protection
Manager\DPM\Volumes\ShadowCopy\FS01\C-8d2a01f3-4b01-11d9-b735-806e6f6e6963\ReplicaDir\Sales“
C:\Sales
```

Führen Sie folgenden Befehl aus, um die richtigen Pfadinformationen wiederherzustellen und den ursprünglichen Inhalt von **C:\Sales** zu löschen.

```
FsPathMerge.exe –FS „C:\Sales\Programme\Microsoft Data Protection
Manager\DPM\Volumes\ShadowCopy\FS01\C-8d2a01f3-4b01-11d9-b735-806e6f6e6963\ReplicaDir\Sales“
C:\Sales -Y
```

Wiederherstellen eines DPM-Servers

Nach einem Notfall können Sie einen DPM-Server wiederherstellen. Dazu müssen Sie zunächst Betriebssystem, Systemstatus und Anwendungen wiederherstellen (einschließlich DPM und dessen Abhängigkeiten). Danach können Sie die DPM-Datenbanken und dann die Replikate wiederherstellen.

Ausführliche Informationen zum Wiederherstellen eines Servers finden Sie im Microsoft TechNet-Artikel „Disaster Recovery“ (http://go.microsoft.com/fwlink/?LinkId=51980, in englischer Sprache).

Hinweis

Für den Fall, dass nur ein Teil der von DPM benötigten Daten beschädigt wurde, müssen Sie zunächst die Volumes mit den Systemdateien für DPM, SQL Server und SQL Server Reporting Services und anschließend die DPM-Datenbanken und Replikate wiederherstellen.

Wiederherstellen von Datenbanken

Verwenden Sie das Programm **DpmSync.exe**, um die DPM- und Berichtsdatenbanken wiederherzustellen. Das Programm befindet sich auf dem SPM-Server im Ordner **\Programme\Microsoft Data Protection Manager\DPM\bin**.

Verwenden von DpmSync zum Wiederherstellen von Datenbanken

DpmSync ist ein Befehlszeilenprogramm, das es Ihnen ermöglicht, die DPM-Datenbank mit dem Status der Datenträger im Speicherpool und mit den installierten Datei-Agents zu synchronisieren. DpmSync stellt die DPM-Datenbanken wieder her, synchronisiert die DPM-Datenbanken mit den Replikaten im Speicherpool, stellt die Berichtsdatenbanken wieder her und weist fehlende Replikate neu zu.

Wenn Sie den DPM-Server von der DPM Evaluation Edition auf DPM 2006 aktualisiert haben, stellen Sie sicher, dass für das Konto MICROSOFTDPMACCT die Berechtigung Vollzugriff für den DPM-Installationsordner **DPMDB** festgelegt ist, bevor sie DpmSync ausführen. Den DPMDB-Installationspfad finden Sie in der Registrierung unter **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Setup\DatabasePath**. Der Standardspeicherort ist **\Programme\Microsoft Data Protection Manager\DPM\DPMDB**.

DpmSync-Syntax

DpmSync **-Sync**

DpmSync **-DpmDbLoc** *Speicherort*

DpmSync **-DpmReportDbLoc** *Speicherort*

DpmSync **-ReallocateReplica**

DpmSync **-?**

Parameter

Parameter	Beschreibung
-Sync	Synchronisiert wiederhergestellte Datenbanken und weist fehlende Replikatvolumes neu zu. Nach der Wiederherstellung von Datenbanken müssen Sie **DpmSync –sync** ausführen. Nachdem Sie **DpmSync –sync** ausgeführt haben, sind einige Replikate möglicherweise noch als fehlend gekennzeichnet. Entfernen Sie im Aufgabenbereich **Verwaltung** in der Tabelle **Datenträger** die fehlenden Datenträger aus DPM, und führen Sie **DpmSync -reallocatereplica** aus, um die als fehlend gekennzeichneten Replikate neu zuzuweisen.
-DpmDbLoc *Speicherort*	Identifiziert den Speicherplatz der DPM-Datenbanksicherung.
-DpmReportDbLoc *Speicherort*	Identifiziert den Speicherplatz der Berichtsdatenbanksicherung.
-ReallocateReplica	Ordnet alle fehlenden Replikatvolumes ohne Synchronisierung neu zu.
-?	Beschreibt die Verwendung des Befehls.

Beispiel

Führen Sie folgenden Befehl aus, um die DPM- und Berichtsdatenbanken aus einem lokalen Sicherungsmedium auf dem DPM-Server wiederherzustellen:

```
DpmSync -DpmDbLoc G:\DPM\Backups\2005\November\DPMDB.bak
DpmSync -DpmReportDbLoc G:\DPM\Backups\2005\November\ReportServer.bak
```

Nach dem Wiederherstellen der DPM- und Berichtsdatenbanken führen Sie folgenden Befehl aus, um die Datenbanken zu synchronisieren:

```
DpmSync -Sync
```

Hinweis

Wenn der DPM-Server in Microsoft Operations Manager 2005 (MOM) überwacht wird, müssen Sie nach der Wiederherstellung der DPM-Datenbank die Warnmeldungen in MOM mit denen des DPM-Servers synchronisieren. Weitere Informationen finden Sie im *Data Protection Manager 2006 Management Pack-Handbuch* auf der TechNet-Website MOM 2005 Management Pack Guides (http://go.microsoft.com/fwlink/?linkid=50206, in englischer Sprache).

Nach dem Wiederherstellen und Synchronisieren der DPM- und Berichtsdatenbanken und bevor Sie die Replikate wiederherstellen, führen Sie folgenden Befehl aus, um den Replikaten Festplattenspeicherplatz zuzuweisen.

```
DpmSync -ReallocateReplica
```

Wiederherstellen von Replikaten

Wenn Sie die Datenbanken wiederherstellen, werden gleichzeitig die Schutzgruppen wiederhergestellt. Der Festplattenspeicherplatz des Speicherpools wird jedoch nicht den wiederhergestellten Schutzgruppen zugewiesen. Bevor Sie die Replikate für die Schutzgruppen wiederherstellen, müssen Sie zunächst den Festplattenspeicherplatz neu zuweisen, der die Replikate und das Übertragungsprotokoll enthalten soll.

Sie können den Speicherplatz für die Replikate entweder in der DPM-Verwaltungskonsole im Dialogfeld **Datenträgerzuordnung ändern** neu zuweisen oder alternativ das DpmSync-Tool mit dem Parameter **-ReallocateReplica** ausführen. Anweisungen für das Zuweisen über die Konsole finden Sie in der DPM-Hilfe unter „How to modify disk allocation“ (http://go.microsoft.com/fwlink/?LinkId=51981, in englischer Sprache). Nachdem Sie den Replikaten neuen Speicherplatz zugewiesen haben, können Sie die Replikate wie folgt auf dem DPM-Server wiederherstellen:

So stellen Sie Replikate wieder her

1. Stellen Sie mit Ihrer Sicherungssoftware die Replikatdaten von Band wieder her.

   Hinweis

   Stellen Sie die Replikate an einem anderen Speicherort wieder her, wenn Sie von einer Bandsicherungskopie des Dateiservers wiederherstellen oder wenn die Sicherungs- und Wiederherstellungshierarchien der Replikate geändert wurden. Wählen Sie als Speicherort für die Wiederherstellung den Ordner **ReplicaDir** aus, der im Aufgabenbereich **Schutz** der DPM-Verwaltungskonsole für das Replikatvolume angegeben ist.

2. Führen Sie einen der folgenden Schritte aus:

   - Wenn die Sicherung mit DpmBackup ausgeführt und der GUID des geschützten Volume seit der Sicherung nicht geändert wurde, führen Sie DpmPathMerge aus, um überflüssige Pfadinformationen zu löschen, und fahren Sie anschließend mit Schritt 3 fort.
   - Wenn die Sicherung mit DpmBackup ausgeführt und der GUID des geschützten Volume seit der Sicherung geändert wurde, führen Sie FsPathMerge aus, um überflüssige Pfadinformationen zu löschen, und fahren Sie anschließend mit Schritt 3 fort.
   - Wenn die Sicherung nicht mit DpmBackup ausgeführt wurde und die Sicherungs- und Replikatordnerhierarchien nicht übereinstimmen, führen Sie FsPathMerge aus, um überflüssige Pfadinformationen zu löschen, und fahren Sie anschließend mit Schritt 3 fort.
   - Wenn die Sicherung nicht mit DpmBackup ausgeführt und die Sicherungs- und die Replikatordnerhierarchien übereinstimmen, fahren Sie mit Schritt 3 fort.

3. Erstellen Sie eine Schattenkopie des wiederhergestellten Replikats. Anweisungen für das manuelle Erstellen einer Schattenkopie finden Sie in der DPM-Hilfe unter „How to Create a Shadow Copy“ (http://go.microsoft.com/fwlink/?LinkId=51982, in englischer Sprache).

   Das Erstellen einer Schattenkopie zu diesem Zeitpunkt bietet Ihnen die Möglichkeit, das Volume bei Bedarf auf dem Dateiserver wiederherzustellen, bevor eine Synchronisierung mit Konsistenzprüfung ausgeführt wird.

4. Führen Sie eine Synchronisierung mit Konsistenzprüfung aus.

   Wenn auch der Dateiserver wiederhergestellt werden muss, führen Sie die Synchronisierung mit Konsistenzprüfung erst aus, nachdem die Dateien auf dem Dateiserver wiederhergestellt wurden.

   Wichtig

   Führen Sie die Konsistenzprüfung für Replikate in der Schutzgruppe erst aus, nachdem alle Replikate in der Schutzgruppe wiederhergestellt wurden.

Verwenden von DpmPathMerge zum Reparieren von Pfaden

Wenn die Bandsicherung, von der die Daten wiederhergestellt wurden, mit DpmBackup erstellt und der GUID des geschützten Volume seit der Sicherung nicht geändert wurde, führen Sie DpmPathMerge aus, um überflüssige Pfadinformationen zu löschen.

Hinweis

Im Gegensatz zur Vorgehensweise unter „Verwenden von FsPathMerge zum Reparieren von Pfaden auf einem DPM-Server“, bei der FsPathMerge für jedes Replikat ausgeführt wird, muss DpmPathMerge nur einmal für alle Replikate auf einem DPM-Server ausgeführt werden.

Bevor Sie DpmPathMerge ausführen, müssen Sie die Dienste DPM-Datei-Agent (**msdpmreplicaagent.exe**) und DPM (**msdpm.exe**) anhalten. Anderenfalls können einige der Replikatdateien gesperrt sein, und der Vorgang schlägt fehl.

Wenn bei dem Befehl **DpmPathMerge** die Meldung „Zugriff verweigert“ zurückgegeben wird, bedeutet dies, dass eine Anwendung ein Dateihandle geöffnet hat oder dass der Ordner **ReplicaDir** schreibgeschützt ist.

DpmPathMerge benötigt auf dem DPM-Server Rechte als Administrator bzw. Sicherungs-Operator.

Informationen zur Problembehandlung für DpmPathMerge finden Sie in diesem Handbuch im Kapitel „Problembehandlung“ (http://go.microsoft.com/fwlink/?LinkId=46369).

DpmPathMerge-Syntax

DpmPathMerge **–DPM**

DpmPathMerge **-?**

Parameter

Parameter	Beschreibung
-DPM	Löscht überflüssige Pfadinformationen aus den Replikatordnern nach einer Wiederherstellung von Band.
-?	Beschreibt die Verwendung des Befehls.

Verwenden von FsPathMerge zum Reparieren von Pfaden auf einem DPM-Server

In der Regel muss FsPathMerge nur dann zum Reparieren von Pfaden verwendet werden, wenn die Wiederherstellung vom Band direkt auf einem geschützten Dateiserver erfolgt. Darüber hinaus müssen Sie in den folgenden Situationen FsPathMerge auf einem DPM-Server ausführen:

- Sie stellen ein Replikat wieder her, bei dem die Sicherungs- und Replikatordnerhierarchien nicht übereinstimmen und die Sicherungskopie nicht mit DpmBackup erstellt wurde.
- Die Sicherungskopie wurde mit DpmBackup erstellt, und der GUID des geschützten Volume wurde seit dem Erstellen der Sicherungskopie geändert.

Wenn der GUID des geschützten Dateiservervolume nicht geändert wurde, wählen Sie den Stamm des Volume, auf dem das Replikatvolume gehostet wird, als Speicherort für die Wiederherstellung der Bandsicherung aus. Die Daten werden dann in dem Verzeichnis wiederhergestellt, aus dem sie gesichert wurden.

Beispiel

- Ursprüngliche Sicherungshierarchie:

  C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01**C-8d2a01f3-4b01-11d9-b735-806e6f6e6963**\ReplicaDir\Sales

- Nach Ändern des GUID des geschützten Dateiservervolume lautet die Hierarchie des Replikatvolume:

  C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01**C-8175ee13-a398-4029-b96c-5ad4504c77c0**\ReplicaDir\Sales

- Wenn die Daten von Band wiederhergestellt werden, ergibt sich als Datenverzeichnis auf dem DPM-Server:

  C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01**C-8175ee13-a398-4029-b96c-5ad4504c77c0**\ReplicaDir\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01**C-8d2a01f3-4b01-11d9-b735-806e6f6e6963**\ReplicaDir\Sales

Um den Pfad zu reparieren, führen Sie FsPathMerge wie folgt aus:

FsPathMerge.exe –FS „C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01**C-8175ee13-a398-4029-b96c-5ad4504c77c0**\ReplicaDir\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01**C-8d2a01f3-4b01-11d9-b735-806e6f6e6963**\ReplicaDir\Sales“ „C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01**C-8175ee13-a398-4029-b96c-5ad4504c77c0**\ReplicaDir\Sales“

Sie können jetzt die Synchronisierung mit Konsistenzprüfung durchführen.

Hinweis
Windows-Tools können keine Pfade anzeigen, die mehr als 256 Zeichen enthalten. Entnehmen Sie die Pfadinformationen den Sicherungsprotokollen, wenn Sie FsPathMerge zum Reparieren von Pfaden verwenden.
Weitere Informationen zu Pfadeinschränkungen finden Sie im Microsoft Knowledge Base-Artikel 177665 „Fehler: "Pfad ist zu lang" bei Überschreiten von MAX_PATH“ (http://go.microsoft.com/fwlink/?LinkId=51995).

Weitere Informationen zu FsPathMerge finden Sie in diesem Kapitel im Abschnitt „Verwenden von FsPathMerge zum Reparieren von Pfaden auf Dateiservern“.

Wiederherstellen eines DPM-Servers auf einem neuen Computer

Sie können eine DPM-Serverkonfiguration auf einem anderen Computer wiederherstellen, etwa im Falle eines Hardwarefehlers oder um DPM-Vorgänge auf einen neuen Computer zu übertragen. Um DPM ordnungsgemäß ausführen zu können, müssen Sie jedoch einige zusätzliche Schritte ausführen.

Sie richten z. B. einen neuen Computer mit dem gleichen Computernamen ein und installieren DPM sowie die gesamte erforderliche Software auf dem neuen Computer. Anschließend stellen Sie die DPM- und Berichtsdatenbanken wieder her, die von einem anderen Computer gesichert wurden. Sie führen DpmSync aus, um die Datenbanken zu synchronisieren. Wenn Sie die DPM-Verwaltungskonsole öffnen, werden folgende Warnungen angezeigt:

• Alle Datenträger fehlen

• Schutz / Replikate fehlen

• Keine Agenten erreichbar

Um das Wiederherstellen von DPM auf einem neuen Computer abzuschließen, müssen Sie diese Probleme wie folgt beheben.

So stellen Sie fehlende Datenträger wieder her

1. Entfernen Sie die fehlenden Datenträger (des ursprünglichen Computers) aus dem Speicherpool. Weitere Informationen finden Sie in der DPM-Hilfe unter „How to remove a disk from the storage pool“ (http://go.microsoft.com/fwlink/?LinkId=51983, in englischer Sprache).
2. Fügen Sie dem Speicherpool einen neuen Datenträgersatz (verbunden mit dem neuen Computer) hinzu. Weitere Informationen finden Sie in der DPM-Hilfe unter „How to add a disk to the storage pool“ (http://go.microsoft.com/fwlink/?LinkId=51985, in englischer Sprache).

So stellen Sie fehlende Replikate wieder her

1. Weisen Sie nacheinander jedes Replikat in der DPM-Verwaltungskonsole neu zu. Weitere Informationen finden Sie in der DPM-Hilfe unter „How to review pending members“ (http://go.microsoft.com/fwlink/?LinkId=51986, in englischer Sprache).

   – oder –

   Führen Sie **DpmSync -ReallocateReplica** aus, um alle fehlenden Replikate mit einem Befehl neu zuzuweisen. Weitere Informationen finden Sie in diesem Kapitel im Abschnitt „Verwenden von DpmSync zum Wiederherstellen von Datenbanken“.
2. Stellen Sie die gesicherten Daten von Band in den neu zugewiesenen Replikaten wieder her. Weitere Informationen zu diesem Vorgang finden Sie in der Dokumentation Ihrer Sicherungssoftware.

So stellen Sie die Kommunikation mit Agenten her

1. Deinstallieren Sie den DPM-Datei-Agent lokal auf jedem Dateiserver. Weitere Informationen finden Sie in der DPM-Hilfe unter "How to uninstall a file agent" (http://go.microsoft.com/fwlink/?LinkId=51987, in englischer Sprache).
2. Wenn der Datei-Agent weiterhin im Aufgabenbereich **Verwaltung** auf der Registerkarte **Agents** angezeigt wird, klicken Sie auf **Informationen aktualisieren**, um den Agent-Datensatz aus der Anzeige zu entfernen.
3. Installieren Sie die Agents über die DPM-Verwaltungskonsole im Aufgabenbereich **Verwaltung** neu. Weitere Informationen finden Sie in der DPM-Hilfe unter „How to install a file agent“ (http://go.microsoft.com/fwlink/?LinkId=51988, in englischer Sprache).
4. Führen Sie für jedes Replikat eine Synchronisierung mit Konsistenzprüfung aus. Weitere Informationen finden Sie in der DPM-Hilfe unter „How to synchronize a replica“ (http://go.microsoft.com/fwlink/?linkid=51910, in englischer Sprache).

KAPITEL 6

Problembehandlung

In diesem Kapitel finden Sie Anleitungen zum Beheben von Schutz- und Wiederherstellungsproblemen in Microsoft System Center Data Protection Manager 2006 (DPM). Das Kapitel ergänzt die DPM-Hilfe sowie das *Planungs- und Bereitstellungshandbuch von DPM*. Im ersten Teil des Kapitels werden allgemeine Verfahren erläutert, auf die in den nachfolgenden Verfahren verwiesen wird. Im zweiten Teil des Kapitels werden Verfahren zur Behebung spezifischer Probleme erläutert.

In diesem Kapitel

Standardverfahren zur Problembehandlung

- Überprüfen des Status eines DPM-Dienstes
- Überprüfen der Namensauflösung
- Erkennen von DNS-Fehlern
- Beheben von „Zugriff verweigert“-Fehlern

Behandeln von Problemen bei der DPM-Installation

Behandeln von Problemen bei der Installation des Datei-Agents

Behandeln von Problemen beim Schutz von Daten

- Behandeln von allgemeinen Problemen beim Schutz von Daten
- Behandeln von Problemen beim manuellen Erstellen von Replikaten

Behandeln von Datenwiederherstellungsproblemen

- Behandeln von allgemeinen Datenwiederherstellungsproblemen
- Behandeln von Problemen beim Konfigurieren der Endbenutzerwiederherstellung
- Behandeln von Problemen bei der Endbenutzerwiederherstellung
- Behandeln von Problemen bei der Endbenutzerwiederherstellung und DFS

Behandeln von Problemen bei der Berichterstellung

Behandeln von Leistungsproblemen

- Behandeln von Problemen bei ungenügendem Arbeitsspeicher
- Behandeln von Problemen mit der CPU-Auslastung
- Behandeln von Problemen mit der Warteschlangenlänge des Datenträgers

Behandeln von Datenbankproblemen

Behandeln von Problemen beim Archivieren und Wiederherstellen von DPM

- Behandeln von Problemen mit DpmBackup und DPM Writer
- Behandeln von Problemen mit FsPathMerge
- Behandeln von Problemen mit DpmPathMerge

Standardverfahren zur Problembehandlung

In diesem Abschnitt finden Sie grundlegende Verfahren zur Problembehandlung, auf die in den folgenden Abschnitten dieses Kapitels verwiesen wird. In diesem Abschnitt werden folgende Verfahren erläutert:

• Überprüfen des Status des DPM-Dienstes

• Überprüfen der Namensauflösung

• Erkennen von DNS-Fehlern

• Beheben von „Zugriff verweigert“-Fehlern

Überprüfen des Status des DPM-Dienstes

Der DPM-Dienst wird nur für die Verarbeitung von DPM-Aufträgen ausgeführt und nach Abschluss eines Auftrags automatisch angehalten. Führen Sie folgende Schritte aus, wenn Sie bei der Problembehandlung angewiesen werden, den Status des DPM-Dienstes zu überprüfen.

So überprüfen Sie den Status des DPM-Dienstes

1. Öffnen Sie auf dem DPM-Server unter **Verwaltung** das Dialogfeld **Dienste**.
2. Klicken Sie unter **Dienste** im Detailbereich mit der rechten Maustaste auf dem DPM-Dienst, und klicken Sie dann auf **Eigenschaften**.
3. Vergewissern Sie sich, dass auf der Registerkarte **Allgemein** für **Starttyp** die Option **Automatisch** ausgewählt ist.
4. Um den Dienst zu starten, klicken Sie auf der Registerkarte **Allgemein** auf **Start**.

   Bei erfolgreichem Start des DPM-Dienstes wird auf der Registerkarte **Allgemein** als Dienststatus **Gestartet** angezeigt. Wenn der DPM-Dienst ordnungsgemäß ausgeführt wird, sollten geplante Schutzaufträge und andere DPM-Aufträge gestartet werden.
5. Wenn der DPM-Dienst nicht gestartet wird, suchen Sie in der Ereignisanzeige von Windows nach Hinweisen auf beendete Dienste, auf die DPM angewiesen ist. Suchen Sie nach folgenden Diensten:
   - DPM-Datei-Agent
   - SQLAgent$MICROSOFT$DPM$ (SQL-Agent)
   - MSSQL$MICROSOFT$DPM$ (SQL Server)
   - Dienst für virtuelle Datenträger (Virtual Disk Service, VDS)
   - Volumeschattenkopie-Dienst (Volume Shadow Copy Service, VSS)
6. Wenn in einem Ereignis das Beenden eines dieser Dienste angezeigt wird, starten Sie den Dienst neu, und vergewissern Sie sich, das für **Starttyp** die Option **Automatisch** ausgewählt ist.
7. Wenn das Problem nicht durch Aktivieren der deaktivierten Dienste aus Schritt 5 behoben werden kann, führen Sie einen Neustart einzelner Dienste durch:
   a. Beenden Sie die Dienste einzeln in dieser Reihenfolge: VDS, VSS, SQL-Agent, SQL Server. Der DPM-Dienst wird automatisch beendet.
   b. Starten Sie den VSS-Dienst.
   c. Starten Sie den DPM-Dienst. Wenn der DPM-Dienst erfolgreich gestartet wird, werden alle abhängigen Dienste – VDS, SQL-Agent und SQL Server – ebenfalls neu gestartet.
8. Wenn der DPM-Dienst immer noch nicht gestartet wird, starten Sie das Microsoft Windows Server 2003-Betriebssystem neu.

   Wenn das Problem nicht durch einen Neustart des Servers behoben werden kann, ist möglicherweise ein Datenbankfehler die Ursache für das Beenden des DPM-Dienstes. Informationen zur Problembehandlung bei Datenbankfehlern finden Sie im Abschnitt „Behandeln von Datenbankproblemen“ in diesem Kapitel.
9. Wenn das Problem durch keinen dieser Lösungsansätze behoben werden kann, wenden Sie sich an den Microsoft Software Service. Weitere Informationen finden Sie auf der Microsoft-Website Hilfe und Support (http://go.microsoft.com/fwlink/?linkid=45276).

Überprüfen der Namensauflösung

Befolgen Sie dieses Verfahren, wenn Sie in den Anweisungen zur Problembehandlung aufgefordert werden, die Namensauflösung zu überprüfen.

So überprüfen Sie die Namensauflösung

1. Führen Sie auf dem Dateiserver den Befehl **ipconfig** aus. Notieren Sie das DNS-Suffix (Domain Name System) und die IP-Adresse (Internet Protocol).
2. Führen Sie auf dem DPM-Server einen **ping**-Befehl mit dem Dateiservernamen aus, um zu überprüfen, ob der Servername in den korrekten vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) und die korrekte IP-Adresse aufgelöst wird.
3. Führen Sie auf dem DPM-Server den Befehl **ipconfig** aus. Notieren Sie das DNS-Suffix und die IP-Adresse.
4. Führen Sie auf dem Dateiserver einen **ping**-Befehl mit dem DPM-Servernamen aus, um zu überprüfen, ob der Servername in den korrekten FQDN und die korrekte IP-Adresse aufgelöst wird.

   Wenn die mit dem Befehlen **ping** und **ipconfig** ermittelten Informationen für den Dateiserver oder den DPM-Server nicht korrekt sind, überprüfen Sie die DNS-Clienteinstellungen auf dem entsprechenden Server.

   Hinweis

   Informationen zum Verwenden des **ping**-Befehls finden Sie in der Hilfe zu Windows Server 2003 unter „Verwenden des ping-Befehls“ (http://go.microsoft.com/fwlink/?LinkId=50821). Informationen zum Verwenden des **ipconfig**-Befehls finden Sie in der Hilfe zu Windows Server 2003 unter „Ipconfig“ (http://go.microsoft.com/fwlink/?LinkId=50823, in englischer Sprache).

Erkennen von DNS-Fehlern

Der DPM-Server und die von ihm geschützten Dateiserver können nur zuverlässig kommunizieren, wenn DNS ordnungsgemäß arbeitet. Mit folgenden Verfahren können Sie DNS-Probleme auf dem DPM-Server oder einem geschützten Dateiserver erkennen und beheben:

- Prüfen Sie in der Konsole **Dienste** den Status folgender Dienste, und starten Sie die Dienste, wenn sie nicht ausgeführt werden:
  - DNS-Client
  - TCP/IP-NetBIOS-Hilfsprogramm (wenn im Intranet NetBIOS verwendet wird)
- Stellen Sie sicher, dass die Hosts-Datei vorhanden und der korrekte Pfad zu dieser Datei konfiguriert ist.
  - Stellen Sie sicher, dass **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ REG_EXPAND_SZ: DataBasePath** auf **%SystemRoot%\System32\drivers\etc** festgelegt ist.
- Stellen Sie sicher, dass sich die Hosts-Datei unter **%SystemRoot%\System32\drivers\etc\hosts** befindet.

- Leeren Sie folgende Caches:
  - Führen Sie **ipconfig /flushdns** aus, um den DNS-Cache zu leeren.
  - Führen Sie **nbtstat -R** und **nbtstat -RR** aus, um den NetBIOS-Cache zu leeren.
  - Führen Sie **arp –d *** aus, um den ARP-Cache (Address Resolution Protocol) zu leeren.
- Überprüfen Sie die IP-Adressen der DNS- und WINS-Server:
  - Führen Sie **ipconfig /ALL** aus, um die IP-Adressen zu ermitteln.
  - Überprüfen Sie die Netzwerkkonnektivität zu jeder dieser IP-Adressen mit den Befehlen **Ping** und **Tracert**.
- Öffnen Sie in Microsoft Management Console (MMC) das Snap-In Gruppenrichtlinienobjekt-Editor für den lokalen Computer, und überprüfen Sie die lokalen DNS-Clienteinstellungen unter **Richtlinie für "Lokaler Computer"\Computerkonfiguration\Administrative Vorlagen\Netzwerk\DNS-Client**.
- Führen Sie **ipconfig /ALL** aus, um die DNS-Suffixsuchliste zu überprüfen.
- Überprüfen Sie die entsprechenden Einstellungen in der Systemsteuerung unter **Netzwerkverbindungen**.
  - Klicken Sie mit der rechten Maustaste auf die Netzwerkverbindung für das LAN, und klicken Sie anschließend auf **Eigenschaften**.
  - Wählen Sie **Internetprotokoll (TCP/IP)** aus, und klicken Sie auf **Eigenschaften**.
  - Klicken Sie im Dialogfeld **Internetprotokolleigenschaften (TCP/IP)** auf die Schaltfläche **Erweitert**.
  - Überprüfen Sie die Einstellungen auf den Registerkarten **DNS** und **WINS**.
- Führen Sie **nslookup** mit den Optionen **debug** und **verbose** aus, um ausführliche Informationen zu den DNS-Abfragen anzuzeigen.
- Bestimmen Sie mit Netzwerkmonitor, ob die richtigen DNS-Server auf Pinganforderungen reagieren.

Weitere Ressourcen

Weitere Informationen zur Problembehandlung bei DNS finden Sie unter:

- Domain Name System Center (http://go.microsoft.com/fwlink/?LinkId=50838, in englischer Sprache)
- How DNS Works (http://go.microsoft.com/fwlink/?LinkId=50839, in englischer Sprache)
- Troubleshooting DNS (http://go.microsoft.com/fwlink/?LinkId=50840, in englischer Sprache)

Tools

Weitere Informationen zu folgenden Tools finden Sie unter „TCP/IP Tools and Settings“ (http://go.microsoft.com/fwlink/?LinkId=50841, in englischer Sprache).

- **Arp:** Anzeigen und Verwalten des ARP-Cache für die Schnittstellen des lokalen Computers.
- **Ipconfig**: Anzeigen der aktuellen TCP/IP-Netzwerkkonfiguration, Aktualisieren oder Freigeben von zugewiesenen DHCP-Leases (Dynamic Host Configuration Protocol) sowie Anzeigen, Registrieren oder Leeren von DNS-Namen.

- **Nbtstat**: Überprüfen des Status aktueller NetBIOS über TCP/IP-Verbindungen (auch bezeichnet als NetBT), Anzeigen und Aktualisieren des NetBIOS-Namenscache sowie Festlegen der mit WINS registrierten Namen.
- **Nslookup**: Überprüfen von Datensätzen, Domänenhostaliasen und -diensten sowie Betriebssysteminformationen durch DNS-Serverabfragen.
- **Ping**: Senden von ICMP-Echomeldungen (ICMP – Internet Control Message Protocol) zum Überprüfen der IP-Konnektivität. Windows Server 2003 fügt dem **ping**-Befehl **IPv6**-Parameter hinzu.
- **Tracert**: Verfolgen eines Pfades bis zu seinem Ziel. Windows Server 2003 fügt dem **tracert**-Befehl **IPv6**-Parameter hinzu.

Beheben von „Zugriff verweigert“-Fehlern

„Zugriff verweigert“-Fehler während der Durchführung von DPM-Aufgaben, für die eine Kommunikation mit einem geschützten Dateiserver erforderlich ist, deuten häufig auf ein Konfigurationsproblem auf dem Dateiserver hin. Wenn während einer Aufgabe, die eine Kommunikation mit den Dateiservern erfordert, ein „Zugriff verweigert“-Fehler auftritt,

führen Sie folgende Schritte aus:

- Stellen Sie sicher, dass die Systemzeit des DPM-Servers und des Dateiservers mit der Systemzeit des Domänencontrollers synchronisiert werden.
- Überprüfen Sie auf einem Dateiserver, auf dem Windows Server 2003 SP1 ausgeführt wird, dass der DPM-Server ein Mitglied der DCOM-Benutzergruppe ist und diese Gruppe über Start- und Zugriffsberechtigungen für DCOM auf dem Dateiserver verfügt.

So überprüfen Sie die Gruppenmitgliedschaft auf einem Dateiserver:

1. Erweitern Sie unter **Computerverwaltung** den Eintrag **System**, erweitern Sie **Lokale Benutzer und Gruppen**, und klicken Sie auf **Gruppen**.
2. Doppelklicken Sie im Detailbereich auf die Gruppe **DCOM-Benutzer**.
3. Vergewissern Sie sich, dass das Computerkonto des DPM-Servers ein Mitglied dieser Gruppe ist.

So überprüfen Sie die Start- und Zugriffsberechtigungen für DCOM auf dem Dateiserver:

1. Öffnen Sie unter **Verwaltung** die Anzeige **Komponentendienste**.
2. Erweitern Sie **Komponentendienste**, erweitern Sie **Computer**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **COM-Security** (COM-Sicherheit) unter **Zugriffsberechtigungen** auf **Edit Limits** (Beschränkungen bearbeiten).
4. Stellen Sie sicher, dass die DCOM-Benutzergruppe über lokale und Remotezugriffsberechtigungen verfügt.
5. Klicken Sie auf der Registerkarte **COM-Security** (COM-Sicherheit) unter **Launch and Activation Permissions** (Start- und Aktivierungsberechtigungen) auf **Edit Limits** (Beschränkungen bearbeiten).
6. Vergewissern Sie sich, dass die DCOM-Benutzergruppe über folgende Berechtigungen verfügt:
   - Lokaler Start
   - Remotestart
   - Lokale Aktivierung
   - Remoteaktivierung

Problembehandlung bei der DPM-Installation

In Tabelle 6.1 finden Sie Hinweise zur Behandlung von Problemen, die bei der Installation von DPM auftreten können. Diese Hinweise ergänzen das Kapitel „Installieren von DPM“ im *Planungs- und Bereitstellungshandbuch von DPM 2006* (http://go.microsoft.com/fwlink/?LinkId=46357, in englischer Sprache).

Tabelle 6.1 DPM-Installationsprobleme

Problem	Details
Nicht-DPM-Anwendungen werden durch die DPM-Installation unterbrochen.	Während der DPM-Installation startet Setup den WMI-Dienst (Windows Management Instrumentation – Windows-Verwaltungsintrumentation) neu. Werden auf dem DPM-Computer andere Anwendungen als DPM und dafür erforderliche Software ausgeführt, werden diese Anwendungen möglicherweise unterbrochen, während der WMI-Dienst neu gestartet wird. Beenden Sie vor der Ausführung von DPM-Setup alle anderen Anwendungen, um eine Unterbrechung zu vermeiden.

Im DPM-Setup wird Fehler 812 angezeigt.
 	
Fehler:
 	
`Konfiguration der Berichte ist fehlgeschlagen. Stellen Sie sicher, dass Microsoft SQL Server Reporting Services ordnungsgemäß installiert sind und ausgeführt werden. ID: 812.`
 	
In der Protokolldatei **DpmSetup.log** wird diese Ausnahmebeschreibung gespeichert:
 	
`The request failed with HTTP status 404.`
	Dieses Problem tritt auf, wenn SQL Server™ Reporting Services und Windows SharePoint Services im selben Anwendungspool von IIS (Internet Information Services) installiert sind.
	
	Gehen Sie folgendermaßen vor, um das Problem zu lösen:
	
	• Deinstallieren Sie die SharePoint Services in der Systemsteuerung mithilfe der Option **Software**. Deinstallieren Sie DPM, und installieren Sie anschließend DPM neu.
	
	– oder –
	
	• Konfigurieren Sie eine parallele Installation von SQL Server Reporting Services und Windows SharePoint Services. Anweisungen hierzu finden Sie unter „Troubleshooting a Side-by-Side Installation of Reporting Services and Windows SharePoint Services“ (http://go.microsoft.com/fwlink/?LinkId=50877, in englischer Sprache).
	
	Hinweis
	Das in diesem Artikel beschriebene Rsactivate-Tool befindet sich im DPM-Installationsverzeichnis unter **Microsoft Data Protection Manager\Prerequisites\MSSQL\Reporting Services\ReportServer\RSReportServer.config**.

Ein im Dialogfeld **Datenträger zum Speicherpool hinzufügen** als verfügbar angezeigter Datenträger wird im Detailbereich als fehlend gekennzeichnet, und die Warnung **Datenträger fehlt** wird angezeigt.	Wenn Sie einen im Speicherpool vorhandenen Datenträger vor der erneuten Zuweisung oder dem Entfernen aus dem Speicherpool löschen oder bereinigen, wird DPM das Fehlen dieses Datenträgers im Speicherpool protokollieren. Wenn Sie anschließend den gelöschten oder bereinigten Datenträger zum Speicherpool hinzufügen, werden für denselben Datenträger zwei Einträge im Speicherpool angezeigt. **Um dieses Problem zu vermeiden**, sollten Sie Datenträger aus dem Speicherpool entfernen, bevor Sie diese löschen oder formatieren. **Um dieses Problem zu beheben**, entfernen Sie in der DPM-Verwaltungskonsole den „fehlenden“ Datenträger, und fügen Sie den „anderen“ Datenträger zum Speicherpool hinzu. Stellen Sie vor dem Entfernen des „fehlenden“ Datenträgers sicher, dass die mit dem im Speicherpool angezeigten Datenträger verbundenen Volumes von Ihnen gelöscht und einem anderen Datenträger zugewiesen wurden.
Beim Versuch, das Snap-In Microsoft Data Protection Manager to zu Microsoft Management Console (MMC) hinzuzufügen, erhalten Sie die Fehlermeldung: Die DPM 2006-Verwaltungskonsole kann nicht geladen werden, weil .NET Framework 1.0 auf dem System installiert ist. .NET Framework 1.0 muss deinstalliert werden, damit die Verwaltungskonsole geladen werden kann.	Die DPM-Administratorkonsole verwendet das mit Windows Server 2003 installierte .NET Framework 1.1. Der hier beschriebene Fehler kann auftreten, wenn ein MMC-Snap-In installiert wurde, das .NET Framework 1.0 enthält und installiert. Um dieses Problem zu lösen, deinstallieren Sie Microsoft .NET Framework über die Systemsteuerung mit der Option **Software**.

Behandeln von Problemen bei der Installation des Datei-Agents

In Tabelle 6.2 finden Sie ergänzende Hinweise zur Problembehandlung bei Fehlermeldungen, die möglicherweise bei der Installation des Datei-Agents auftreten.

Tabelle 6.2 Probleme bei der Installation des Datei-Agents

Fehlermeldung	Mögliche Ursache	Problembehandlung
300: Fehler bei Agent-Vorgang. Kommunikation mit dem angegebenen Server nicht möglich.	• Konfiguration der Firewall auf dem Dateiserver • RPC (Remote Procedure Call) ist nicht verfügbar	Siehe: • Das in diesem Handbuch enthaltene Kapitel „Verwalten von Servern“ zu den Anforderungen an die Firewallkonfiguration. • Microsoft Knowledge Base-Artikel 224370 „Troubleshooting RPC Server is Unavailable in Windows“ (http://go.microsoft.com/fwlink/?LinkId=45817, in englischer Sprache).
303: Der Agent-Vorgang am angegebenen Server ist fehlgeschlagen.	• Auf dem angegebenen Server wird eine andere Installation ausgeführt. • Das Startvolume des Dateiservers ist als FAT-Dateisystem formatiert.	• Warten Sie auf den Abschluss der Installation, und wiederholen Sie anschließend den Vorgang. • Konvertieren Sie das Startvolume nach NTFS, wenn ausreichend Speicherplatz verfügbar ist. Weitere Informationen über die Verwendung des **Convert**-Befehls zum Konvertieren von FAT-Volumes nach NTFS finden Sie im Microsoft TechNet-Artikel „Convert“ (http://go.microsoft.com/fwlink/?LinkId=50882, in englischer Sprache). Lesen Sie auch den Microsoft Knowledge Base-Artikel 156560 „Free Space Required to Convert FAT to NTFS“ (http://go.microsoft.com/fwlink/?LinkId=50883, in englischer Sprache). • Wenn diese Schritte das Problem nicht lösen können, starten Sie den Server neu, und wiederholen Sie den Vorgang.

306: Fehler bei der Agent-Installation, weil auf dem angegebenen Server bereits eine andere Version des DPM-Datei-Agents installiert ist.	Dieses Problem tritt auf, wenn der Datei-Agent bereits auf einem Dateiserver installiert ist, die DPM-Datenbank jedoch keinen Datensatz über die Installation des Datei-Agents enthält.	1. Deinstallieren Sie den Datei-Agent lokal auf dem Dateiserver. 2. Klicken Sie auf dem DPM-Server in der DPM-Verwaltungskonsole im Aufgabenbereich **Verwaltung** auf die Registerkarte **Agents**, wählen Sie den Dateiserver aus, und klicken Sie anschließend im Bereich **Aktionen** auf **Informationen aktualisieren**. Der Status des Agents wird zu **Fehler** geändert. 3. Klicken Sie im Detailbereich auf **Entfernt den Dateiservereintrag auf diesem DPM-Computer**. 4. Installieren Sie den Datei-Agent auf dem Dateiserver neu. Anweisungen hierzu finden Sie in der DPM-Hilfe unter „Managing Agents“ (http://go.microsoft.com/fwlink/?linkid=51976, in englischer Sprache).
308: Fehler bei Agent-Vorgang. Es ist ein Fehler bei der Kommunikation mit dem DPM-Datei-Agent-Dienst auf dem angegebenen Server aufgetreten.	• Konfiguration der Firewall auf dem Dateiserver • IPSec (Internet Protocol Security) • RPC ist nicht verfügbar	• Lesen Sie das in diesem Handbuch enthaltene Kapitel „Verwalten von Servern“ zu den Anforderungen an die Firewallkonfiguration. • IPsec ist möglicherweise zum Sperren bestimmten IP-Datenverkehrs konfiguriert, bspw. auf einem bestimmten Port oder zu bestimmten Adressen. Lesen Sie zur Behandlung von IPsec-Problemen „IPsec Troubleshooting“ (http://go.microsoft.com/fwlink/?LinkId=50885, in englischer Sprache). • Microsoft Knowledge Base-Artikel 224370 „Troubleshooting RPC Server is Unavailable in Windows“ (http://go.microsoft.com/fwlink/?linkid=45817, in englischer Sprache).
316: Fehler bei Agent-Vorgang. Der DPM-Datei-Agent-Dienst auf dem angegebenen Server antwortet nicht.	Konfiguration der Firewall auf dem DPM-Server	Lesen Sie das in diesem Handbuch enthaltene Kapitel „Verwalten von Servern“ zu den Anforderungen an die Firewallkonfiguration.
319: Fehler bei Agent-Vorgang. Bei der Kommunikation mit dem DPM-Agent-Koordinator-Dienst auf dem angegebenen Server ist ein Fehler aufgetreten.	Konfiguration der Firewall auf dem Dateiserver	Lesen Sie das in diesem Handbuch enthaltene Kapitel „Verwalten von Servern“ zu den Anforderungen an die Firewallkonfiguration.

324: Fehler bei Agent-Vorgang. Der DPM-Agent-Koordinator-Dienst auf dem angegebenen Server reagiert nicht.	Konfiguration der Firewall auf dem DPM-Server	Lesen Sie das in diesem Handbuch enthaltene Kapitel „Verwalten von Servern“ zu den Anforderungen an die Firewallkonfiguration.
329: Der Agent-Vorgang ist fehlgeschlagen. Die Version von Quota Advisor, die auf dem angegebenen Server installiert ist, ist nicht kompatibel. Installieren Sie Quota Advisor, Version 5.3.2190.2 oder höher, oder deinstallieren Sie Quota Advisor auf dem Server. Falls Quota Advisor von einem OEM installiert wurde, wenden Sie sich an den OEM-Support.	DPM kann keine Dateiserver schützen, auf denen **QAFilter.sys**, Version 5.3.2190.0 oder früher, ausgeführt wird. **QAFilter.sys** ist eine Komponente der Produkte Veritas Storage Exec, Veritas Storage CeNTral, WQuinn Storage Manager und WQuinn QuotaAdvisor.	DPM kann den Datei-Agent nicht auf Servern installieren, auf denen eine nicht unterstützte Version von **QAFilter.sys** ausgeführt wird. Installieren Sie nach der Installation des Datei-Agents keine nicht unterstütze Version von **QAFilter.sys** auf einem geschützten Dateiserver. Wenn eine der folgenden Bedingungen auf Ihren Server zutrifft, wird auf ihm eine nicht unterstützte Version von **QAFilter.sys** ausgeführt: • Beim Dateiserver handelt es sich um einen Windows Storage Server oder ein von Windows unterstütztes NAS-Gerät, auf dem ein Quota-Feature auf Benutzer- oder Verzeichnisebene installiert ist, das eine ältere Version als 5.3.2190.0 aufweist. • Auf dem Dateiserver wird eine Version von Storage Exec oder Storage CeNTral ausgeführt, die eine frühere Version als 5.3.2190.2 von QuotaAdvisor installiert hat. **Hinweis** DPM gestattet das Abschließen der Agent-Installation ab Version 5.3.2190.0, offiziell unterstützt werden jedoch lediglich Versionen ab 5.3.2190.2. • Informationen zum Erhalt eines Hotfix, der DPM das Schützen eines Windows Storage Server oder eines NAS-Geräts mit Storage Manager ermöglicht, finden Sie im Microsoft Knowledge Base-Artikel 896718 (http://go.microsoft.com/fwlink/?LinkId=50886, in englischer Sprache).

341: Fehler bei Agent-Vorgang. Die angegebenen Anmeldeinformationen verfügen nicht über ausreichende Berechtigungen auf dem angegebenen Server.	• Das verwendete Konto verfügt auf dem Dateiserver nicht über ausreichende Berechtigungen. • Da die Systemzeiten auf dem DPM-Server, dem Dateiserver und dem Domänencontroller nicht synchronisiert sind, schlägt die Kerberos-Authentifizierung fehl. • Die DNS-Einstellungen auf dem DPM-Server sind fehlerhaft.	• Wiederholen Sie den Vorgang mit einem Konto, das über Administratorberechtigungen auf dem angegebenen Server verfügt. • Stellen Sie sicher, dass die Systemzeiten des DPM-Servers und des Dateiservers mit der Systemzeit des Domänencontrollers synchronisiert werden. • Überprüfen Sie die DNS-Einstellungen. Informationen finden Sie in diesen Kapitel unter „Erkennen von DNS-Fehlern“.
342: Fehler bei Agent-Vorgang. Kommunikation mit dem angegebenen Server nicht möglich.	Konfiguration der Firewall auf dem Dateiserver	Lesen Sie das in diesem Handbuch enthaltene Kapitel „Verwalten von Servern“ zu den Anforderungen an die Firewallkonfiguration.
348: Fehler beim Versuch, mit dem DPM-Agent-Koordinatordienst auf dem angegebenen Server zu kommunizieren.	Sicherheit des COM-Objekts auf dem Dateiserver	Überprüfen Sie die COM-Berechtigungen auf dem Dateiserver. Anweisungen hierzu finden Sie in diesem Kapitel unter „Beheben von „Zugriff verweigert“-Fehlern“.

Behandeln von Problemen beim Schutz von Daten

Dieser Abschnitt enthält Informationen zur Problembehandlung für die folgenden Bereiche des Schutzes von Daten:

• Allgemeine Probleme beim Schutz von Daten

• Manuelles Erstellen von Replikaten

Behandeln von allgemeinen Problemen beim Schutz von Daten

Tabelle 6.3 enthält Richtlinien zur Problembehandlung beim Schutz von Daten. Diese Richtlinien ergänzen die Informationen in der DPM-Hilfe (http://go.microsoft.com/fwlink/?linkid=46350) sowie das Kapitel „Planing Data Protection“ im *Planing and Deployment Guide von DPM 2006* (http://go.microsoft.com/fwlink/?LinkId=46356, in englischer Sprache).

Tabelle 6.3 Schutzprobleme

Problem	Details
DPM kann nicht mehr mit den geschützten Servern kommunizieren.	Der DPM-Computer wurde möglicherweise vorübergehend von der Active Directory-Domäne getrennt, der er angehört. Der DPM-Computer kann bspw. aufgrund einer fehlerhaften Vertrauensstellung für Arbeitsstation und Domäne getrennt worden sein. Wenn der DPM-Computer erneut gestartet wird, wird er mit demselben Namen neu mit der Domäne verbunden, er erhält jedoch eine neue SID (Security Identifier). Alle durch diesen DPM-Computer geschützten Dateiserver verfügen über eine DCOM-Sicherheitseinstellung in der Agent-Registrierung, die die alte SID enthält. Aus diesem Grund können die Dateiserver weder den DPM-Datei-Agent starten noch die Kommunikation mit dem DPM-Computer fortsetzen. **So stellen Sie die Kommunikation und die Aktivitäten zum Schutz von Daten wieder her** 1. Deinstallieren Sie den Datei-Agent lokal auf dem Dateiserver. 2. Klicken Sie auf dem DPM-Server in der DPM-Verwaltungskonsole im Aufgabenbereich **Verwaltung** auf die Registerkarte **Agents**, wählen Sie den Dateiserver aus, und klicken Sie anschließend im Bereich **Aktionen** auf **Informationen aktualisieren**. Der Status des Agents wird zu **Fehler** geändert. 3. Klicken Sie im Detailbereich auf **Entfernt den Dateiservereintrag auf diesem DPM-Computer**. 4. Installieren Sie den Datei-Agent auf dem Dateiserver neu. Anweisungen hierzu finden Sie in der DPM-Hilfe unter „Managing agents“ (http://go.microsoft.com/fwlink/?linkid=51976, in englischer Sprache).

Sie installieren den Datei-Agent auf einem Dateiserver, führen anschließend den Assistenten **Neue Schutzgruppe** aus, können jedoch nicht auf Freigaben oder Volumes auf dem Dateiserver zugreifen.	Wenn Sie einen Datei-Agent installieren, kann es nach einem erneuten Starten des Dateiservers bis zu 20 Minuten dauern, ehe der Datei-Agent für die Beantwortung von Anfragen des Assistenten **Neue Schutzgruppe** zur Verfügung steht. Sie können nach einem erneuten Starten des Dateiservers 20 Minuten bis zur erneuten Ausführung des Assistenten warten, oder den folgenden Schritt ausführen: 1. Öffnen Sie in der DPM-Verwaltungskonsole den Aufgabenbereich **Verwaltung**. 2. Klicken Sie auf die Registerkarte **Agents**, und klicken Sie anschließend im Bereich **Aktionen** auf **Informationen aktualisieren**.
Die Konsistenzprüfung scheint die Daten wesentlich langsamer als die Replikaterstellung zu übertragen.	Eine Konsistenzprüfung führt eine Überprüfung auf Dateibasis durch, um sicherzustellen, dass alle replizierten Daten konsistent mit den geschützten Daten sind, dabei werden alle vom Replikat abweichenden Daten übertragen. Während der Konsistenzprüfung zeigt die Fortschrittsanzeige jedoch lediglich die Menge der übertragenen Daten an. Da lediglich geänderte Daten übertragen werden, können Sie aus der Fortschrittsanzeige nicht auf die Geschwindigkeit der Konsistenzprüfung schließen.
Die Zeit der Schattenkopie stimmt nicht mit der Synchronisierungszeit überein.	Beim Erstellen einer Schattenkopie wird die Zeit der letzten Änderung auf dem geschützten Volume berücksichtigt. **Beispiel**: Sie möchten die Erstellung einer Schattenkopie um 11 Uhr veranlassen. Die letzte Änderung auf dem geschützten Volume wurde gegen 8:30 Uhr vorgenommen. Die um 11 Uhr erstellte Schattenkopie wird einen Zeitstempel von 8:30 Uhr aufweisen.
Die Synchronisierung schlägt mit dem Fehler 42 fehlt: DPM konnte nicht mit dem DPM-Datei-Agent auf auf dem angegebenen Server kommunizieren, da der Zugriff verweigert wurde.	Zusätzlich zu den in der Fehlermeldung aufgelisteten Ursachen kann dieser Fehler auch unter folgenden Bedingungen auftreten: • Der Agent wurde auf einem Dateiserver unter Windows Server 2003 SP1 lokal deinstalliert. • Ein Dateiserver unter Windows 2000 Server wurde auf Windows Server 2003 SP1 aktualisiert.

Synchronisierungsaufträge schlagen fehl, die Einträge im Anwendungsereignisprotokoll enthalten die Information: „Unable to connect to Active Directory.“	Mögliche Lösungswege: • Wiederholen Sie den Auftrag. • Überprüfen Sie die Netzwerkkonnektivität zwischen DPM-Server und Domänencontroller. • Stellen Sie sicher, dass DPM ein Mitglied der Domäne ist und dass der Domänencontroller ausgeführt wird. • Überprüfen Sie die Zugriffsrechte des DPM-Servers für das Aktualisieren von Active Directory: a. Öffnen Sie das Snap-In Active Directory-Benutzer und -Computer, und stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Funktionen** ausgewählt ist. b. Erweitern Sie die Domäne, anschließend **System**. c. Klicken Sie mit der rechten Maustaste auf **MS-ShareMapConfiguration** (MS-ShareMap-Konfiguration), und klicken Sie anschließend auf **Eigenschaften**. • Überprüfen Sie auf der Registerkarte **Sicherheit** das Vorhandensein des DPM-Servernamens.

Die AutoErmittlung kann Änderungen der Freigaben nicht erkennen.	Wenn eine Freigabe auf einem Dateiserver geschützt ist und der Dateiserver gleichzeitig eine nicht unterstützte Freigabe enthält, kann die AutoErmittlung Änderungen der Freigaben, z. B. neue, entfernte oder neu zugewiesene Freigaben, auf diesem Dateiserver nicht erkennen. „Ausstehende Mitglieder“ werden von der AutoErmittlung auf einem Dateiserver mit einer geschützten Freigabe nicht erkannt, wenn der Dateiserver gleichzeitig eine Freigabe mit einem der folgenden nicht unterstützten Typen als Ziel enthält: • FAT-Volume • CD-ROM-Laufwerk • USB-Laufwerk • Bereitstellungspunkt innerhalb eines anderen Bereitstellungspunktes • Ordner mit Sonderfunktionen: Ordner „System Volume Information“, „RECYCLER“ • Nicht unterstützter Analysepunkt (jeder von einem Bereitstellungspunkt abweichender Analysepunkt) • Ein Ordner auf einem System mit Unterscheidung zwischen Groß- und Kleinschreibung, der einen lediglich in der Schreibweise abweichenden Namen wie ein anderer Ordner im übergeordneten Ordner hat (z. B. „F:\MarketingDocs“ und „F:\marketingdocs“) • Wenn ein Dateiserver eine nicht unterstützte Freigabe aus der Liste enthält, sollten Sie lediglich Ordner und Volumes schützen, damit die AutoErmittlung ordnungsgemäß ausgeführt werden kann.
Nach der Aktualisierung eines Dateiservers von Windows 2000 Server auf Windows Server 2003 SP1 schlagen die Konsistenzprüfungen der geschützten Volumes auf diesem Dateiserver wiederholt fehl.	Nach der Aktualisierung von Windows 2000 Server auf Windows Server 2003 SP1 erhalten die Volumes auf dem Server unter Umständen neue GUIDs. Wenn dieser Fall eintritt, wird das Volume von der AutoErmittlung aufgrund des neuen GUID erkannt, obwohl es bereits geschützt wird. Außerdem wird das Replikat des geschützten Volumes als inkonsistent gekennzeichnet, und die Konsistenzprüfung für dieses Replikat schlägt wiederholt fehl. **Um dieses Problem zu beheben**, deinstallieren Sie in der DPM-Verwaltungskonsole den Datei-Agent auf dem Dateiserver und installieren den Datei-Agent anschließend neu. Diese Vorgehensweise erfordert ein erneutes Starten des Dateiservers.

Behandeln von Problemen beim manuellen Erstellen von Replikaten

Den Prozess der manuellen Replikaterstellung nutzt der Administrator zum Erstellen des ersten Replikats, indem er die Daten von einem Wechselmedium (bspw. einer Bandsicherung) zum DPM-Server überträgt, nicht jedoch über das Netzwerk vom Dateiserver zum DPM-Server. Dieser Vorgang entspricht der Wiederherstellung eines Replikats auf einem DPM-Server von einer Bandsicherung und wird in diesem Handbuch im Kapitel „Archivieren und Wiederherstellen von Daten“ (http://go.microsoft.com/fwlink/?LinkId=46368) erläutert.

Die jeweils erforderlichen Schritte zum Erstellen eines manuellen Replikats sind von der zur Datenübertragung verwendeten Sicherungssoftware abhängig. Informationen über die Verwendung von Sicherungsprodukten mit DPM sowie Whitepapers mit entsprechenden Richtlinien finden Sie im Bereich Featured Technical Content auf der DPM-Produktwebsite (http://go.microsoft.com/fwlink?linkid=33686, in englischer Sprache).

Beim Erstellen eines manuellen Replikats muss insbesondere auf eine Beibehaltung der Verzeichnisstruktur und Eigenschaften (Zeitstempel und Sicherheitsberechtigungen) entsprechend den zu schützenden Daten geachtet werden. Anweisungen zur Auswahl der spezifischen Einstellungen finden Sie in der Dokumentation Ihrer Sicherungssoftware und in den Whitepapers im Bereich Featured Technical Content auf der DPM-Produktwebsite.

Wenn das Replikat ordnungsgemäß erstellt wird, entspricht die Verzeichnisstruktur des Replikatordners **ReplicaDir** auf dem DPM-Server exakt der Verzeichnisstruktur des zu schützenden Volumes.

Während einer manuellen Replikaterstellung können ggf. folgende Fehler auftreten:

- **Übertragen der Daten in eine flache Verzeichnisstruktur** – Der vollständige Pfad der auf dem geschützten Dateiserver befindlichen Quelldaten ist nicht enthalten. Das Replikat muss unter Beibehaltung der Pfade der auf dem Dateiserver gespeicherten Daten erstellt werden. Wenn Sie das Replikat mit einem falschen Pfad erstellt haben, löschen Sie die Replikatdaten, und erstellen Sie das Replikat neu. Wenn Sie die Synchronisierung mit Konsistenzprüfung bereits gestartet haben, führen Sie folgende Schritte aus:
    - Entfernen Sie das geschützte Volume oder die geschützte Freigabe aus der Schutzgruppe, und löschen Sie anschließend das Replikat.
    - Fügen Sie das Volume oder die Freigabe der Schutzgruppe hinzu.
    - Erstellen Sie manuell ein neues Replikat.

    Bei einer flachen Verzeichnisstruktur kann die Synchronisierung mit Konsistenzprüfung das gesamte Replikat über das Netzwerk mit dem Dateiserver synchronisieren. Dies belegt wertvolle Bandbreite und CPU-Ressourcen.
- **Übertragen der Daten in ein abweichendes Verzeichnis** – Dies führt zum Erstellen einer fehlerhaften Hierarchie des Replikats. Das Replikat muss an dem Speicherort erstellt werden, der in der DPM-Verwaltungskonsole im Bereich **Eigenschaften** zum Erstellen von manuellen Replikaten festgelegt wurde. Wenn Sie die Daten an einen abweichenden Speicherort übertragen haben, können Sie die Daten mit FsPathMerge verschieben oder die Replikatdaten und das Replikat neu erstellen. Wenn Sie die Synchronisierung mit Konsistenzprüfung bereits gestartet haben, führen Sie folgende Schritte aus:
    - Entfernen Sie das geschützte Volume oder die geschützte Freigabe aus der Schutzgruppe, und löschen Sie anschließend das Replikat.
    - Fügen Sie das Volume oder die Freigabe der Schutzgruppe hinzu.
    - Erstellen Sie manuell ein neues Replikat.

Bei einer abweichenden Replikathierarchie kann die Synchronisierung mit Konsistenzprüfung das gesamte Replikat über das Netzwerk mit dem Dateiserver synchronisieren. Dies belegt wertvolle Bandbreite und CPU-Ressourcen.

- **Erneutes Erstellen von Verknüpfungspunkten** – Es werden neue anstelle der bereits vorhandenen Verknüpfungspunkte verwendet. Dieses Problem kann beim Verwenden einer von einem DPM-Server erstellten Bandsicherung auftreten. Wenn Sie während des Wiederherstellungsvorgangs nicht die Verwendung der vorhandenen Verknüpfungspunkte festlegen, werden die Daten möglicherweise in einem fehlerhaften Pfad wiederhergestellt. Löschen Sie in diesem Fall die Daten und den Pfad manuell, und erstellen Sie dann manuell das Replikat neu.
- **Fehler beim Wiederherstellen der Sicherheitseinstellungen** – Tritt bei der Wiederherstellung auf. Die Datensicherung enthält die Sicherheitseinstellungen der Quelldaten. Wenn Sie die Daten einer Sicherung ohne Sicherheitseinstellungen wiederherstellen, werden die ordnungsgemäßen ACLs (Access Control Lists – Zugriffssteuerungslisten) für die Dateien und Ordner nicht konfiguriert, bis die Synchronisierung mit Konsistenzprüfung erfolgreich beendet wird. Fehlerhafte Sicherheitseinstellungen der Replikatdaten können möglicherweise einen Zugriff auf diese Daten durch nicht berechtigte Benutzer zulassen. Fehler beim Wiederherstellen der Sicherheitseinstellungen führen außerdem zu einer längeren Laufzeit der Synchronisierung mit Konsistenzprüfung und zu unnötigen Datenübertragungen im Netzwerk.
- **Ändern der Zeitstempel für Dateien und Ordner** – Verursacht durch einen Benutzerfehler oder einen Designfehler der verwendeten Sicherungssoftware. Die Sicherungssoftware legt unter Umständen die Zeitstempel der wiederhergestellten Dateien und Ordner auf den Zeitpunkt der Wiederherstellung fest, statt die Zeitstempel zu verwenden, die diese Dateien und Ordner zum Zeitpunkt der Sicherung hatten. Fehlerhafte Zeitstempel führen zu einer längeren Laufzeit der Synchronisierung mit Konsistenzprüfung und zu umfangreicheren Datenübertragungen.

Behandeln von Datenwiederherstellungsproblemen

Dieser Abschnitt enthält Informationen zur Problembehandlung für die folgenden Bereiche der Datenwiederherstellung:

- Allgemeine Datenwiederherstellungsprobleme
- Probleme beim Konfigurieren der Endbenutzerwiederherstellung
- Probleme bei der Endbenutzerwiederherstellung
- Endbenutzerwiederherstellung und DFS

Behandeln von allgemeinen Datenwiederherstellungsproblemen

Tabelle 6.4 enthält Hinweise zur Behandlung von Problemen, die bei der Datenwiederherstellung durch einen Administrator mit der DPM-Verwaltungskonsole auftreten können.

Tabelle 6.4 Allgemeine Datenwiederherstellungsprobleme

Problem	Details
Sie müssen mehrere Dateien zur Wiederherstellung auswählen.	Zum Wiederherstellen mehrerer Dateien in einem einzelnen geschützten Ordner wird die Wiederherstellung des gesamten Ordners anstelle der einzelnen Dateien empfohlen. Das Wiederherstellen einzelner ausgewählter Dateien kann ggf. mehr Zeit in Anspruch nehmen als die Wiederherstellung des gesamten Ordners.
Wenn Sie zur Datenwiederherstellung in der DPM-Verwaltungskonsole den Knoten **Alle geschützten Freigaben** verwenden, reagiert die Benutzeroberfläche nicht mehr.	Wenn Sie mehr als 100 Freigaben schützen, ist die Datenwiederherstellung über den Knoten **Alle geschützten Volumes** schneller. Wenn Sie mehr als 500 Freigaben schützen, wird ausdrücklich eine Datenwiederherstellung über den Knoten **Alle geschützten Volumes** empfohlen. Erweitern Sie den Knoten **Alle geschützten Freigaben** nicht, wenn Sie sehr viele Freigaben schützen. Eine einwandfreie Funktion der DPM-Verwaltungskonsole ist in diesem Fall nicht gewährleistet.
Beim Wiederherstellen komprimierter Dateien weicht die Angabe der übertragenen Bytes im Aufgabenbereich **Überwachung** von den Angaben im Aufgabenbereich **Wiederherstellung** ab.	Im Aufgabenbereich **Wiederherstellung** wird die unkomprimierte Dateigröße angezeigt.
In der Datenwiederherstellung sind keine Analysepunkte enthalten.	Aus Sicherheitsgründen bezieht DPM in Replikaten oder Schattenkopien geschützter Daten keine Analysepunkte mit ein. Nachdem Sie ein Volume, einen Ordner oder eine Freigabe mit einem Analysepunkt wiederhergestellt haben, müssen Sie den Analysepunkt manuell neu erstellen. Sie können jedoch das Ziel eines Analysepunktes genau wie andere Volumes, Ordner oder Freigaben wiederherstellen, sofern das Ziel Mitglied einer Schutzgruppe ist.

Behandeln von Problemen beim Konfigurieren der Endbenutzerwiederherstellung

Tabelle 6.5 enthält Hinweise zur Behandlung von Problemen, die beim Konfigurieren der Endbenutzerwiederherstellung auftreten können.

Tabelle 6.5 Probleme beim Konfigurieren der Endbenutzerwiederherstellung

Problem	Details
Wenn ein Synchronisierungsauftrag ausgeführt wird, nachdem Sie die Endbenutzerwiederherstellung aktiviert oder deaktiviert haben, wird die folgende Warnung angezeigt: Die Berechtigungen, die für die Endbenutzerwiederherstellung auf dem angegebenen Server verwendet werden, konnten nicht aktualisiert werden. Die Aktualisierung der Berechtigungen schlug aus dem folgenden Grund fehl: Der angegebene Server kann nicht durchsucht werden, weil der Host nicht erreicht werden kann. Weitere Informationen finden Sie, wenn Sie die DPM-Verwaltungskonsole öffnen und den Aufgabenbereich „Überwachung“ auswählen.	1. Stellen Sie die Konnektivität zwischen Dateiserver und DPM-Server sicher. Weitere Informationen finden Sie in diesem Kapitel im Abschnitt „Standardverfahren“ unter „Überprüfung der Namensauflösung“ und „Erkennen von DNS-Fehlern“. 2. Synchronisieren Sie die Replikate aller geschützten Volumes des angegebenen Servers.
Beim Konfigurieren der Endbenutzerwiederherstellung wird folgende Fehlermeldung angezeigt: Active Directory konnte nicht konfiguriert werden, weil der DPM-Computer mit dem angegebenen Namen nicht gefunden werden konnte.	1. Führen Sie auf dem DPM-Server einen **ping**-Befehl für den Domänencontroller aus, um die Konnektivität zu überprüfen. 2. Stellen Sie sicher, dass keine aktiven Warnungen in der DPM-Verwaltungskonsole angezeigt werden.

Behandeln von Problemen bei der Endbenutzerwiederherstellung

Tabelle 6.6 enthält Hinweise zur Behandlung von Problemen, die bei der Datenwiederherstellung durch Endbenutzer auftreten können.

Tabelle 6.6 Probleme bei der Endbenutzerwiederherstellung

Problem	Details
Der Endbenutzer kann auf dem DPM-Server nicht auf ältere Dateiversionen zugreifen, ältere Dateiversionen auf dem Dateiserver werden jedoch angezeigt.	Wenn Schattenkopien für freigegebene Ordner auf dem geschützten Dateiserver aktiviert sind, werden auf dem Client für die Endbenutzerwiederherstellung die Schattenkopien auf dem geschützten Dateiserver, nicht jedoch Schattenkopien auf dem DPM-Server angezeigt. Deaktivieren Sie die Schattenkopien für freigegebene Ordner auf dem Dateiserver. Weitere Informationen über Schattenkopien für freigegebene Ordner in Windows Server 2003 finden Sie im Whitepaper „Introduction to Shadow Copies of Shared Folders“ (http://go.microsoft.com/fwlink/?linkid=19622, in englischer Sprache).
Sie können über die Administratorfreigabe nicht auf vorherige Versionen eines Ordners zugreifen. (Sie schützen bspw. **c:\Ordner**, können jedoch keine vorherigen Versionen anzeigen, wenn Sie über **\\server\c$\Ordner** darauf zugreifen.)	DPM unterstützt keinen Zugriff über Administratorfreigaben. Verwenden Sie den Aufgabenbereich **Wiederherstellung** in der DPM-Verwaltungskonsole zum Wiederherstellen des Ordners.
Auf der Registerkarte **Vorherige Versionen** wird nichts angezeigt.	An der Datei wurden keine Änderungen vorgenommen, oder alle in den Snapshots auf dem DPM-Server vorhandenen vorherigen Dateiversionen stimmen mit der Version auf dem Dateiserver überein. Ändern Sie die Datei, und warten Sie eine vollständige Synchronisierung ab, oder überprüfen Sie direkt vorhandene vorherige Versionen des Verzeichnisses.

Die Registerkarte **Vorherige Versionen** ist nicht verfügbar.	**So identifizieren und beheben Sie dieses Problem** 1. Stellen Sie sicher, dass die Schattenkopieclient-Software auf dem Clientcomputer installiert ist. Anweisungen hierzu finden Sie in der DPM-Hilfe unter „How to install the shadow copy client software“ (http://go.microsoft.com/fwlink/?LinkId=52006, in englischer Sprache). 2. Navigieren Sie im Aufgabenbereich **Schutz** oder **Wiederherstellung** der DPM-Verwaltungskonsole zu der Freigabe, und überprüfen Sie das Vorhandensein von Schattenkopien für diese Freigabe. 3. Wenn Sie die Endbenutzerwiederherstellung nach dem Schützen einer Freigabe aktiviert haben, müssen Sie die nächste geplante Konsistenzprüfung abwarten oder eine manuelle Synchronisierung durchführen (mit oder ohne Konsistenzprüfung). Führen Sie den Befehl **net share** aus, und überprüfen Sie die Freigaben, oder verwenden Sie das Element **Freigaben** in der Konsole **Computerverwaltung**. Eine der Dateifreigabe entsprechende Replikatfreigabe sollte angezeigt werden. Replikatfreigaben haben die Bezeichnung „server_share“, wobei „server“ für den Namen des Dateiservers und „share“ für den ursprünglichen Freigabenamen steht. 4. Überprüfen Sie die DNS-Einstellungen auf dem DPM-Server und den Clientcomputern. Stellen Sie sicher, dass diese den DNS-Server kontaktieren können. Weitere Informationen finden Sie in diesem Kapitel unter „Erkennen von DNS-Fehlern“. 5. Stellen Sie sicher, dass der Clientcomputer Mitglied derselben Domäne wie der DPM-Server ist.

Die Endbenutzerwiederherstellung kann für Freigaben fehlschlagen, die zunächst aus Schutzgruppen entfernt und anschließend erneut hinzugefügt wurden.	DPM kann Freigaben eventuell nicht aus Replikaten löschen, wenn die Quellfreigaben bzw. die Volumes, die die Quellfreigaben enthalten, aus Schutzgruppen entfernt wurden und die Option zum Löschen des Replikats und der Schattenkopien aktiviert ist. Wenn Sie eine solche Freigabe erneut einer Schutzgruppe hinzufügen, sind vorherige Versionen der Freigabedaten für die Endbenutzerwiederherstellung nicht verfügbar. Um dieses Problem zu vermeiden, müssen Sie das Löschen der verknüpften Freigabe im Replikat durch DPM sicherstellen, bevor Sie eine vormals geschützte Freigabe erneut zu einer Schutzgruppe auf dem DPM-Server hinzufügen, auf dem die Endbenutzerwiederherstellung aktiviert ist. Wenn die verknüpfte Freigabe nicht gelöscht wurde, löschen Sie die Freigabe manuell. **So identifizieren und löschen Sie eine Freigabe aus einem Replikat** 1. Klicken Sie unter **Verwaltung** auf **Computerverwaltung**. 2. Erweitern Sie **System**, anschließend **Freigegebene Order**, und wählen Sie **Freigaben** aus. Freigaben im Replikat können über ihren Ordnerpfad identifiziert werden: **Programme\Microsoft Data Protection Manager\2006\Volumes\Replica\<dateiserver>\<volume_GUID>\ReplicaDir\<freigabename>**. Verwenden Sie den Volumebuchstaben und den GUID zur Überprüfung, ob die Pfadangabe des Replikats nach wie vor gültig ist. 1. Klicken Sie mit der rechten Maustaste auf die zu löschende Freigabe, und klicken Sie auf **Freigabe beenden**. 2. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Behandeln von Problemen bei der Endbenutzerwiederherstellung und DFS

In einem DFS-Namespace können Verknüpfungen über mehrere Ziele verfügen, die replizierte Daten enthalten. Die durch einen Endbenutzer wiederhergestellte Datei entspricht möglicherweise nicht der erwarteten Dateiversion, wenn Sie mehrere DFS-Ziele schützen.

Der DFS-Namespace **\\public\apps** kann Benutzer z. B. zu den eigentlichen Zielen in **\\public1\apps** und **\\public2\apps** führen. Wenn beide Ziele von DPM geschützt werden und der Benutzer eine Datei aus der DFS-Verknüpfung wiederherstellen möchte, wird im Schattenkopieclient die Schattenkopie der Datei aus dem ersten verfügbaren geschützten Ziel angezeigt. Wenn die Ziele zum Zeitpunkt der Erstellung der Schattenkopie nicht synchronisiert waren, wird der Benutzer unter Umständen eine falsche Version der Datei wiederherstellen.

Wenn Sie lediglich ein Ziel einer DFS-Verknüpfung schützen und der Benutzer eine Datei wiederherstellen möchte, werden die Ziele einer DFS-Verknüpfung vom Schattenkopieclient geprüft, und der Benutzer wird mit dem geschützten und nicht mit dem ersten verfügbaren Ziel verbunden.

Behandeln von Problemen bei der Berichterstellung

Die Tabelle 6.7 enthält eine Anleitung zur Behandlung von Problemen, die möglicherweise beim Konfigurieren, Anzeigen, Exportieren oder Abonnieren von DPM-Berichten auftreten.

Tabelle 6.7 Allgemeine Probleme bei der Berichterstellung

Problem	Details
Sie abonnieren alle 5 Berichte zur Zustellung von E-Mails, es werden jedoch nicht alle Berichte übermittelt.	Wenn ein DPM-Server eine große Anzahl von Dateiservern schützt, sollten Sie den Zeitplan für eine Übermittlung von Berichten per E-Mail zeitlich staffeln. Wenn Ihre Planung eine Übermittlung aller 5 Berichte zur selben Zeit vorsieht, verhindern die Speichereinschränkungen von SQL Server Reporting Services möglicherweise das Senden einiger Berichte.
Die vorgesehenen E-Mail-Empfänger erhalten die Berichte nicht, und von DPM werden keine Fehler erstellt.	Dieses Problem tritt häufig auf, wenn die Zustellung von E-Mails durch die Sicherheitseinstellungen der E-Mail-Empfängeradresse eingeschränkt wird. Das ist zum Beispiel möglicherweise dann der Fall, wenn die Empfängeradresse eine Verteilergruppe ist, deren Eigenschaften so eingerichtet sind, dass nur E-Mails von autorisierten Absendern empfangen werden. Das Problem kann ebenfalls unter folgenden Bedingungen auftreten: • Die E-Mail-Adresse des Empfängers ist ungültig. • Die Absenderadresse für E-Mail-Nachrichten auf der Registerkarte **SMTP Server** ist eine ungültige oder nicht überwachte E-Mail-Adresse. Je nach Ursache des Problems gibt es die folgenden Lösungswege: • Stellen Sie sicher, dass die zum Abonnieren von Berichten verwendeten E-Mail-Adressen gültig sind. • Stellen Sie sicher, dass E-Mail-Benachrichtigungen durch die Sicherheitseinstellungen des E-Mail-Alias oder der Verteilergruppe nicht so eingeschränkt werden, dass eine Übermittlung an die vorgesehenen Adressen nicht möglich ist. • Stellen Sie sicher, dass die Absenderadresse, die auf der Registerkarte **SMTP Server** zur Verwendung in E-Mail-Nachrichten festgelegt ist, eine gültige E-Mail-Adresse enthält. • Weitere Informationen finden Sie unter „How to configure the SMTP server“ (http://go.microsoft.com/fwlink/?linkid=51908, in englischer Sprache) in der DPM-Hilfe.

Beim Exportieren von HTML-Berichten nach MHTML werden Diagramme nicht ordnungsgemäß angezeigt.	Wenn ein Benutzer auf einem DPM-Server unter Windows Server 2003 SP1 einen HTML-Bericht nach Webarchiv (MHTML-Format) exportieren möchte, werden die Diagramme im Bericht nicht angezeigt. Dies ist ein Problem bei Internet Explorer und tritt nur beim ersten Exportieren eines Berichts auf. In den folgenden exportierten Berichten werden die Diagramme ordnungsgemäß angezeigt.
Beim Versuch, einen DPM-Bericht anzuzeigen, werden die Fehlermeldungen „Server wurde nicht gefunden“ oder „DNS-Fehler“ angezeigt, oder der Bericht wird in Internet Explorer nicht angezeigt.	Möglicherweise sind die Proxyservereinstellungen in Internet Explorer nicht korrekt. Um Berichte in Internet Explorer anzuzeigen, muss der Proxyserver für lokale Verbindungen umgangen werden. **So umgehen Sie den Proxyserver für lokale Verbindungen** 1. Klicken Sie in Internet Explorer im Menü **Extras** auf **Internetoptionen**. 2. Klicken Sie auf der Registerkarte **Verbindungen** im Dialogfeld **Internetoptionen** auf **Einstellungen**. 3. Stellen Sie sicher, dass im Dialogfeld **Einstellungen für lokales Netzwerk (LAN)** der korrekte Proxyserver eingetragen ist und das Kontrollkästchen **Proxyserver für lokale Adressen umgehen** aktiviert ist. 4. Wenn die Proxyservereinstellung korrekt ist, das Kontrollkästchen zum Umgehen des Proxyservers für lokale Adressen jedoch aufgrund einer Unternehmensrichtlinie nicht aktiviert werden kann, klicken Sie auf **Erweitert** und fügen den HTTP://DPM-Servernamen zu den Ausnahmen hinzu.
Im Aufgabenbereich **Berichterstellung** der DPM-Verwaltungskonsole werden nicht alle DPM-Berichttypen angezeigt.	Ein Administrator hat eine oder mehrere DPM-Berichtvorlagen manuell vom DPM-Computer entfernt. **So stellen Sie die fehlenden DPM-Berichttypen wieder her** 1. Stellen Sie sicher, dass derzeit keine DPM-Aufträge ausgeführt werden. 2. Schließen Sie die DPM-Verwaltungskonsole. 3. Deinstallieren Sie DPM unter **Software** mit aktivierter Option **Daten beibehalten**. Wenn Sie die Option **Daten beibehalten** nicht aktivieren, wird Ihre vorhandene Konfiguration zum Schutz von Daten gelöscht, einschließlich des Schutzzeitplans, der Replikate und Schattenkopien. 4. Installieren Sie nach dem erfolgreichen Beenden der Deinstallation DPM erneut.

Berichte werden von DPM nicht in die Formate MHTML, Excel oder PDF exportiert.	Wenn die Internet Explorer-Optionen für verstärkte Sicherheit und Secure Socket Layer (SSL) aktiviert sind, kann DPM Berichte nicht in die Formate MHTML, Microsoft Excel oder PDF exportieren. Um Berichte in die Formate MHTML, Excel oder PDF zu exportieren, müssen Sie die Internet Explorer-Option für verstärkte Sicherheit deaktivieren. **So deaktivieren Sie die verstärkte Sicherheitseinstellung von Internet Explorer** 1. Klicken Sie unter **Software** auf **Windows-Komponenten hinzufügen/entfernen**. 2. Deaktivieren Sie im Assistenten für Windows-Komponenten das Kontrollkästchen **Verstärkte Sicherheitskonfiguration für Internet Explorer**.
Ein Bericht enthält keine Daten, wenn Sie ihn mit der DPM-Verwaltungskonsole oder als E-Mail-Anlage anzeigen.	Folgende Ursachen können verhindern, dass der Bericht zum geplanten Zeitpunkt ausgeführt wird: • Die Berichterstellung konnte keine Verbindung zur DPM-Datenbank herstellen. • Der DPM-Computer wurde für Wartungszwecke heruntergefahren. • Der DPM-Computer wurde gerade neu gestartet. Wenn ein Bericht fehlschlägt, wird der Bericht erneut ausgeführt, sobald der Computer wieder online ist oder zum nächsten geplanten Zeitpunkt. Dadurch werden Berichte wieder in der DPM-Verwaltungskonsole angezeigt. So stellen Sie sicher, dass E-Mail-Abonnenten den korrigierten Bericht empfangen 1. Wählen Sie in der DPM-Verwaltungskonsole im Aufgabenbereich **Berichterstellung** den Berichttyp aus. 2. Klicken Sie im Bereich **Aktionen** auf **Zeitplan**. 3. Klicken Sie in der Dropdownliste **Häufigkeit** auf **Einmal**. 4. Wählen Sie in den Dropdownlisten **Datum** und **Uhrzeit** den nächstmöglichen Zeitplan aus. 5. Nach der Erstellung des Berichts „Einmal Ausführen“ wird er an alle Abonnenten gesendet. Legen Sie nach erfolgreichem Senden des Berichts wieder den regulären Zeitplan für die Berichte fest.

Der Administrator wird bei jedem Zugriff auf DPM-Berichte zur Eingabe seiner Anmeldeinformationen aufgefordert.	Der Name des DPM-Computers wird automatisch in Internet Explorer zur Sicherheitszone **Lokales Intranet** hinzugefügt, um den Zugriff auf die DPM-Berichte ohne Eingabe zusätzlicher Anmeldeinformationen zuzulassen. Wenn Sie den Namen des DPM-Computers manuell zur Zone **Vertrauenswürdige Sites** hinzufügen, wird diese Standardeinstellung überschrieben, sodass Internet Explorer zur Eingabe der Anmeldeinformationen auffordert, bevor der Zugriff auf DPM-Berichte gewährt wird. Entfernen Sie den Namen des DPM-Computers aus der Zone **Vertrauenswürdige Sites**, und fügen Sie ihn zur Zone **Lokales Intranet** hinzu. Weitere Informationen über Sicherheitszonen in Internet Explorer finden Sie im Kapitel „Security Zones“ (http://go.microsoft.com/fwlink/?LinkId=52308, in englischer Sprache) in Internet Explorer 6.0 Resource Kit.

Beim Anzeigen von Berichten werden folgende Fehlermeldungen angezeigt:
 	
`Fehler bei der Berichtsverarbeitung. (rsProcessingAborted) Onlinehilfe anzeigen`
 	
`Fehler bei der Anmeldung. (rsProcessingAborted) Onlinehilfe anzeigen`
 	
`Fehler bei der Anmeldung: Der Benutzer ist für den angeforderten Anmeldungstyp auf diesem Computer nicht berechtigt.`
	Um diesen Fehler zu beheben, müssen Sie sicherstellen, dass das DPMReport-Konto über das Benutzerrecht **Lokal anmelden zulassen** verfügt.
	
	So weisen Sie dem DPMReport-Konto das Benutzerrecht „Lokal anmelden zulassen“ zu
	
	1. Öffnen Sie unter **Verwaltung** die Option **Lokale Sicherheitsrichtlinie**.
	2. Erweitern Sie unter **Sicherheitseinstellungen** die Option **Lokale Richtlinien**, und klicken Sie anschließend auf **Zuweisen von Benutzerrechten**.
	3. Klicken Sie mit der rechten Maustaste im Detailbereich auf **Lokal anmelden**, und klicken Sie dann mit der rechten Maustaste auf **Eigenschaften**.
	4. Klicken Sie im Dialogfeld **Eigenschaften von Lokal anmelden** auf **Benutzer oder Gruppe hinzufügen**.
	5. Klicken Sie im Dialogfeld zur Auswahl von Benutzern, Computern oder Gruppen auf **Pfade**, dann auf den Namen des DPM-Servers und anschließend auf **OK**.
	6. Geben Sie im Dialogfeld **Benutzer, Computer oder Gruppen auswählen** die Option **DPMReport** ein, und klicken Sie auf **OK**.
	7. Klicken Sie im Eigenschaftendialogfeld **Lokal anmelden** auf **OK**.
	8. Klicken Sie mit der rechten Maustaste im Detailbereich auf **Lokale Anmeldung verweigern**, und klicken Sie mit der rechten Maustaste auf **Eigenschaften**.
	9. Wenn das DPMReport-Konto aufgeführt ist, wählen Sie **DPMReport** aus, und klicken Sie dann auf **Entfernen**.

Beim Auswählen des Aufgabenbereichs **Berichterstellung** in der DPM-Verwaltungskonsole wird die Fehlermeldung 3013 angezeigt: `Aufgrund von IIS-Konnektivitätsproblemen konnte keine Verbindung zum SQL Server Reporting Services-Server hergestellt werden.`	Dieses Problem kann auftreten, wenn der WWW-Publishingdienst beendet oder die Standardwebsite für diesen Dienst deaktiviert wird. **So beheben Sie diesen Fehler** 1. Vergewissern Sie sich, dass in der Konsole **Dienste** der Status des WWW-Publishingdiensts **Gestartet** ist. Wenn der Dienst nicht gestartet wurde, klicken Sie mit der rechten Maustaste auf den Dienst, und klicken Sie dann auf **Start**. 2. Wenn der Status des WWW-Publishingdiensts **Gestartet** ist oder der Fehler durch Starten des Diensts nicht behoben werden kann, überprüfen Sie den Status der Standardwebsite. **So überprüfen Sie den Status der Standardwebsite** a. Öffnen Sie unter **Verwaltung** den **Internetinformationsdienste-Manager**. b. Klicken Sie im Navigationsbereich auf **Websites**. c. Vergewissern Sie sich, dass im Detailbereich der Status der Standardwebsite **Wird ausgeführt** ist. Andernfalls klicken Sie mit der rechten Maustaste auf **Standardwebsite**, und klicken Sie anschließend auf **Start**. d. Schließen Sie die DPM-Verwaltungskonsole, und öffnen Sie sie anschließend erneut.
Die Datenträgerauslastung für inaktive Replikate wird im Datenträgerauslastungsbericht nicht ordnungsgemäß angezeigt.	Für bestehende Schutzgruppen oder Dateiserver werden unter **Aktuelle Speicherpooldetails für** keine aktuellen Informationen (z. B. bis auf die Minute aktuell) für entfernte, hinzugefügte oder am Tag der Berichterstellung aus dem Schutz entfernte Replikate angezeigt. Die Datenträgerauslastung dieser Replikate wird in Berichten, die mindestens einen Tag nach der Änderung erstellt wurden, ordnungsgemäß angezeigt.
Der Zugriff auf Berichte ist nicht möglich.	Wenn ASP.NET 2.0 nach dem DPM-Setup auf dem DPM-Server installiert wird, arbeitet die DPM-Berichterstellung möglicherweise nicht ordnungsgemäß. **So konfigurieren Sie Reporting Services neu für das Verwenden von .NET Framework 1.1** 1. Öffnen Sie eine Eingabeaufforderung. 2. Geben Sie Folgendes in die Eingabeaufforderung ein: **cd /d %windir%\Microsoft.NET\Framework\v1.1.4322** 3. Geben Sie Folgendes in die Eingabeaufforderung ein: **aspnet_regiis /s W3SVC/1/ROOT/ReportServer** 4. Schließen Sie die DPM-Verwaltungskonsole, und öffnen Sie sie anschließend erneut.

Während des DPM-Setups wird Fehler 812 angezeigt.
 	
Fehler:
 	
`Konfiguration der Berichte ist fehlgeschlagen. Stellen Sie sicher, dass Microsoft SQL Server Reporting Services ordnungsgemäß installiert sind und ausgeführt werden. ID: 812.`
 	
In der Protokolldatei DpmSetup.log wird diese Ausnahmebeschreibung gespeichert:
 	
`Anforderung mit HTTP-Status 404 fehlgeschlagen.`
	Dieses Problem tritt auf, wenn SQL Server™ Reporting Services und Windows SharePoint Services im selben Anwendungspool von IIS (Internet Information Services) installiert sind.
	
	Gehen Sie folgendermaßen vor, um das Problem zu lösen:
	
	• Deinstallieren Sie SharePoint Services über **Software**, deinstallieren Sie DPM, und installieren Sie anschließend DPM erneut.
	
	-oder-
	
	• Konfigurieren Sie eine parallele Installation von SQL Server Reporting Services und Windows SharePoint Services. Weitere Anleitungen finden Sie unter „Troubleshooting a Side-by-Side Installation of Reporting Services and Windows SharePoint Services“ (http://go.microsoft.com/fwlink/?LinkId=50877, in englischer Sprache).
	
	Hinweis
	
	Das unter „Troubleshooting a Side-by-Side Installation of Reporting Services and Windows SharePoint Services“ erläuterte Rsactivate-Tool befindet sich im DPM-Installationspfad unter **Microsoft Data Protection Manager\Prerequisites\MSSQL\Reporting Services\ReportServer\RSReportServer.config**.

Behandeln von Leistungproblemen

Dieser Abschnitt enthält Informationen zur Behandlung der folgenden Leistungsprobleme:

• Ungenügender Arbeitsspeicher

• CPU-Auslastung

• Warteschlangenlänge des Datenträgers

Weitere Informationen über die DPM-Leistung finden Sie im Kapitel „Verwalten der Leistung“ in diesem Handbuch.

Wenn Sie zur DPM-Überwachung Microsoft System Center Data Protection Manager 2006 (DPM) Management Pack verwenden, finden Sie im „Microsoft System Center Data Protection Manager 2006 Management Pack Guide“ (http://go.microsoft.com/fwlink/?linkid=43706, in englischer Sprache) weitere Informationen zum Behandeln von Leistungsproblemen.

Behandeln von Problemen bei ungenügendem Arbeitsspeicher

Wenn die Leistung des DPM-Servers extrem niedrig ist und Sie als Ursache dafür unter anderem ungenügenden Arbeitsspeicher feststellen, führen Sie die folgenden Schritte aus, um das Problem mit ungenügendem Arbeitsspeicher genau zu identifizieren und zu beheben:

So erhalten Sie weitere Informationen zu einem Problem mit ungenügendem Arbeitsspeicher

Verwenden Sie auf dem DPM-Server den Task Manager, um die Prozesse zu ermitteln, die den meisten Speicherplatz in Anspruch nehmen. (Überprüfen Sie die Auslastung des Arbeitsspeichers auf der Registerkarte **Prozesse**.) Wenn diese Prozesse nicht in ihren ordnungsgemäßen Leistungsbereichen ausgeführt werden, müssen möglicherweise zusätzliche anwendungsspezifische Diagnosen zum Feststellen der Ursache durchgeführt werden.

Beachten Sie jedoch, dass die Speicherauslastung für die DPM-Instanz des SQL Server-Diensts (Sqlservr.exe) in der Regel vergleichsweise hoch ist. (Der Benutzername der DPM-Instanz lautet MicrosoftDPMAcct.) Eine hohe Speicherauslastung durch MicrosoftDPMAcct stellt kein Problem dar. Der Dienst verwendet normalerweise eine große Menge an Arbeitsspeicher zum Zwischenspeichern, gibt jedoch bei wenig freiem Arbeitsspeicher diesen wieder frei.

So beheben Sie das Problem sofort

1. Schließen Sie die DPM-Verwaltungskonsole.
2. Sie sollten unter Umständen weniger wichtige DPM-Aufträge abbrechen und später ausführen, wenn mehr Arbeitsspeicher zur Verfügung steht.

   - **Wichtig**

     Das Abbrechen eines Schutzauftrags kann den Schutz der Daten gefährden. Weitere Informationen finden Sie unter „How to cancel a job“ (http://go.microsoft.com/fwlink/?LinkId=52007, in englischer Sprache) in der DPM-Hilfe.
3. Beenden Sie den DPM-Dienst und den SQL Server-Dienst, und starten Sie beide Dienste anschließend erneut. Öffnen Sie unter **Verwaltung** das Dialogfeld **Dienste**, und führen Sie dann die folgenden Schritte aus, um die Dienste neu zu starten:

   a. Beenden Sie den DPM-Dienst, wenn er ausgeführt wird. (Der Dienst wird automatisch beendet, wenn er nicht in Verwendung ist.) Wenn Sie den DPM-Dienst beenden, werden alle aktiven Aufträge abgebrochen.

   b. Beenden Sie den SQL Server-Dienst (MSSQL$Microsoft$DPM$).

   c. Starten Sie den SQL Server-Dienst (MSSQL$Microsoft$DPM$).

   d. Starten Sie den DPM-Dienst neu.

So beheben Sie ein langfristiges Problem mit ungenügendem Arbeitsspeicher aufgrund von DPM-Aufträgen

1. Stellen Sie sicher, dass keine anderen Anwendungen auf dem DPM-Server ausgeführt werden.
2. Ändern Sie die Schutzzeitpläne für die Schutzgruppen, um Schutzaufträge zu staffeln. Eventuell sollten Sie die Synchronisierungsaufträge zeitlich versetzen, sodass diese nicht mehr zur vollen Stunde ausgeführt werden. Weitere Informationen finden Sie unter „How to modify protection options“ (http://go.microsoft.com/fwlink/?LinkId=52008, in englischer Sprache) in der DPM-Hilfe.
3. Wenn aufgrund hoher Arbeitsspeicherauslastung durch DPM-Aufträge weiterhin die Leistung eingeschränkt ist, sollten Sie möglicherweise zusätzlichen Arbeitsspeicher hinzufügen oder einen Teil der Schutzauslastung auf einen anderen DPM-Server übertragen. Informationen über die Arbeitsspeicheranforderungen für einen DPM-Server finden Sie im Kapitel „Planen der Bereitstellung“ im Planungs- und Bereitstellungshandbuch von DPM 2006 (http://go.microsoft.com/fwlink/?LinkId=46355, in englischer Sprache).

Behandeln von Problemen mit der CPU-Auslastung

Wenn die Leistung des DPM-Servers extrem niedrig ist, und Sie als Ursache die CPU-Auslastung feststellen, führen Sie die folgenden Schritte aus, um den CPU-Engpass zu identifizieren und zu beheben:

So erhalten Sie weitere Informationen zur CPU-Auslastung

Verwenden Sie auf dem DPM-Server den Task Manager, um die Prozesse zu ermitteln, die die meiste Verarbeitungskapazität in Anspruch nehmen. (Überprüfen Sie die CPU-Auslastung auf der Registerkarte **Prozesse**.) Wenn diese Prozesse nicht in ihren ordnungsgemäßen Leistungsbereichen ausgeführt werden, müssen möglicherweise zusätzliche anwendungsspezifische Diagnosen zum Feststellen der Ursache durchgeführt werden.

So beheben Sie das Problem sofort

1. Schließen Sie die DPM-Verwaltungskonsole.
2. Sie sollten unter Umständen weniger wichtige DPM-Aufträge abbrechen und später ausführen, wenn mehr Arbeitsspeicher zur Verfügung steht.

   - **Wichtig**

     Das Abbrechen eines Schutzauftrags kann den Schutz der Daten gefährden. Weitere Informationen finden Sie unter „How to cancel a job“ (http://go.microsoft.com/fwlink/?LinkId=52007, in englischer Sprache) in der DPM-Hilfe.
3. Beenden Sie den DPM-Dienst und den SQL Server-Dienst, und starten Sie beide Dienste anschließend erneut. Öffnen Sie unter **Verwaltung** das Dialogfeld **Dienste**, und führen Sie dann die folgenden Schritte aus, um die Dienste neu zu starten:

   a. Beenden Sie den DPM-Dienst, wenn er ausgeführt wird. (Der Dienst wird automatisch beendet, wenn er nicht in Verwendung ist.) Wenn Sie den DPM-Dienst beenden, werden alle aktiven Aufträge abgebrochen.

   b. Beenden Sie den SQL Server-Dienst (MSSQL$Microsoft$DPM$).

   c. Starten Sie den SQL Server-Dienst (MSSQL$Microsoft$DPM$).

   d. Starten Sie den DPM-Dienst neu.

So beheben Sie ein langfristiges Problem mit CPU-Engpässen aufgrund von DPM-Aufträgen

1. Deaktivieren Sie die Komprimierung über das Netzwerk für die Schutzgruppen. Dies ist eine erweiterte Schutzoption, die für einzelne Schutzgruppen konfiguriert werden kann. Weitere Informationen finden Sie unter „How to modify protection options“ (http://go.microsoft.com/fwlink/?linkid=52008, in englischer Sprache) in der DPM-Hilfe. Das Deaktivieren der Komprimierung über das Netzwerk kann eine höhere Netzwerkauslastung verursachen. Wenn für das Ausführen von Schutzaufträgen innerhalb eines WAN (Wide Area Network) eine Komprimierung über das Netzwerk erforderlich ist, müssen Sie aufgrund der zusätzlichen CPU-Auslastung möglicherweise die Hardware aktualisieren.
2. Ändern Sie die Schutzzeitpläne für die Schutzgruppen, um Schutzaufträge zu staffeln. Eventuell sollten Sie die Synchronisierungsaufträge zeitlich versetzen, sodass diese nicht mehr zur vollen Stunde ausgeführt werden. Weitere Informationen finden Sie unter „How to modify protection options“ (http://go.microsoft.com/fwlink/?linkid=52008, in englischer Sprache) in der DPM-Hilfe.
3. Wenn aufgrund der CPU-Auslastung weiterhin die Leistung eingeschränkt ist, müssen Sie möglicherweise entweder die Hardware aktualisieren oder einen Teil der Schutzauslastung auf einen anderen DPM-Server übertragen.

   Informationen über die Prozessoranforderungen für einen DPM-Server finden Sie im Kapitel „Planing a Deployment“ im Planning and Deployment Guide von DPM 2006 (http://go.microsoft.com/fwlink/?LinkId=46355, in englischer Sprache).

Behandeln von Problemen mit der Warteschlangenlänge des Datenträgers

Wenn die Leistung des DPM-Servers extrem niedrig ist, und Sie niedrige Datenträgerleistung als Ursache feststellen, führen Sie folgende Schritte aus, um die Warteschlange des Datenträgers zu reduzieren.

So erhalten Sie weitere Informationen zur Leistung von Datenträgerressourcen

Um Datenträgerengpässe auf dem DPM-Server zu identifizieren, müssen Sie neben der Datenträgerauslastung, dem Datenträgerdurchsatz und der Auslagerungsmenge auch die Muster der Datenträgerwarteschlange analysieren.

- Weitere Informationen zum Analysieren der Datenträgerleistung auf einem Computer, auf dem ein Microsoft Windows-Betriebssystem ausgeführt wird, finden Sie im Kapitel „Examining and Tuning Disk Performance“ (http://go.microsoft.com/fwlink/?LinkId=46520, in englischer Sprache) im Serverbetriebshandbuch des Microsoft Windows 2000 Server Resource Kit.
- Informationen zum Optimieren der Datenträgerleistung auf einem Computer, auf dem ein Microsoft Windows Server 2003-Betriebssystem ausgeführt wird, finden Sie unter „Solving performance problems“ in Windows Server 2003 Hilfe und Support (in englischer Sprache).

So beheben Sie das Problem sofort

1. Sie sollten unter Umständen weniger wichtige DPM-Aufträge abbrechen und später ausführen, wenn mehr Arbeitsspeicher zur Verfügung steht.

   Wichtig

   Das Abbrechen eines Schutzauftrags kann den Schutz der Daten gefährden. Weitere Informationen finden Sie unter „How to cancel a job“ (http://go.microsoft.com/fwlink/?LinkId=52007, in englischer Sprache) in der DPM-Hilfe.

2. Starten Sie den DPM-Datei-Agent auf dem DPM-Server neu, wenn der Bedarf an Datenträgerressourcen nicht geringer wird. Öffnen Sie unter **Verwaltung** das Dialogfeld **Dienste**. Klicken Sie dann mit der rechten Maustaste auf **DPM-Datei-Agent**, und klicken Sie auf **Neu starten**. Wenn Sie den DPM-Dienst neu starten, werden alle aktiven Aufträge abgebrochen.

So beheben Sie ein langfristiges Problem mit der Datenträgerleistung aufgrund von DPM-Aufträgen

1. Optimieren Sie die Datenträgerleistung auf dem DPM-Server. Weitere Informationen finden Sie unter „Solving performance problems“ in Windows Server 2003 Hilfe und Support (in englischer Sprache).
2. Ändern Sie die Schutzzeitpläne für die Schutzgruppen, um Schutzaufträge zu staffeln. Eventuell sollten Sie die Synchronisierungsaufträge zeitlich versetzen, sodass diese nicht mehr zur vollen Stunde ausgeführt werden. Möglicherweise sollten Sie auch die Anzahl der Schattenkopieaufträge im Schutzzeitplan reduzieren. Weitere Informationen zum Ändern der Schutzzeitpläne finden Sie unter „How to modify protection options“ (http://go.microsoft.com/fwlink/?linkid=52008, in englischer Sprache) in der DPM-Hilfe.
3. Wenn die DPM-Leistung aufgrund der Datenträgerleistung weiterhin eingeschränkt wird, muss möglicherweise die Hardware aktualisiert werden. Informationen zum Planen der Datenträgerkonfiguration in einem DPM-Speicherpool finden Sie im Kapitel „Planen einer Bereitstellung“ im Planungs- und Bereitstellungshandbuch von DPM 2006 (http://go.microsoft.com/fwlink/?LinkId=46355, in englischer Sprache).
4. Überprüfen Sie die Konfiguration der Antivirussoftware auf dem DPM-Server. Weitere Information finden Sie im Kapitel „Verwalten von Servern“ in diesem Handbuch (http://go.microsoft.com/fwlink/?LinkId=46367).

Behandeln von Datenbankproblemen

DPM-Prozesse beruhen auf Datenbanken, die in Microsoft SQL Server erstellt wurden:

- In der DPM-Datenbank (DPMDB.mdf) werden DPM-Einstellungen und Konfigurationsinformationen gespeichert.
- In der Berichtdatenbank (ReportServer.mdf) werden Berichterstellungsinformationen für DPM gespeichert.

Außerdem beruhen DPM-Prozesse auf folgende Datenbanken: Tempdb.mdf, Master.mdf, Model.mdf und Msdb.mdf.

Datenbankfehler können ein Fehlschlagen von DPM-Aufträgen verursachen, sich auf die Verwendung der DPM-Verwaltungskonsole auswirken, die DPM-Berichterstellung verhindern und den DPM-Dienst anhalten. Ein durch nicht genügend Arbeitsspeicher oder hohe CPU-Auslastung verursachter Rückstand an Abfragen kann außerdem eine Zeitüberschreitung des Clients verursachen (wenn DPM-Prozesse eine lange Zeit für das Herstellen einer SQL-Abfrage oder Verbindung zu SQL Server benötigen).

Datenbankfehler können u. a. durch folgende Gründe verursacht werden:

- Eine ungewöhnlich hohe Anzahl an Schutzaufträgen wird gleichzeitig auf dem DPM-Server verarbeitet, und SQL Server kann die Abfragen nicht rechtzeitig bearbeiten. Dies ist der häufigste Grund für Zeitüberschreitungen des Clients und allgemeine Netzwerkfehler.
- Ein von DPM verwendetes Datenbank- oder Transaktionsprotokoll verfügt nicht mehr über genügend Speicherplatz.
- Eine von DPM verwendete Datenbank ist in einen inkonsistenten Zustand eingetreten oder wurde beschädigt.
- Der SQL Server-Dienst wird nicht ausgeführt oder ist nicht ordnungsgemäß konfiguriert.

Einige Datenbankfehler in DPM werden durch vorübergehende Probleme ausgelöst, die sich möglicherweise von selbst beheben. Beispiele für diese Probleme sind unzureichende Ressourcen, Zeitüberschreitungen des Clients, ungenügender Speicherplatz für Transaktionsprotokolle, SQL Server-Deadlocks, wiederherstellbare Datenbankfehler und Probleme mit Zeitplänen.

Bevor Sie für diesen Datenbankfehlertyp Diagnosen ausführen, befolgen Sie die folgenden Schritte auf dem DPM-Server, um sich zu vergewissern, dass das Problem nicht vorübergehend ist.

So beheben Sie Probleme, die vorübergehende Datenbankfehler verursachen können

1. Stellen Sie sicher, dass der SQL Server-Dienst ausgeführt wird. Öffnen Sie unter **Verwaltung** das Dialogfeld **Dienste**, und vergewissern Sie sich, dass der Status des Diensts MSSQL$Microsoft$DPM$ **Gestartet** ist. Wenn dies nicht der Fall ist, klicken Sie mit der rechten Maustaste auf den Dienst, und klicken Sie entweder auf **Start** oder auf **Fortsetzen**.
2. Wenn das Problem dadurch nicht behoben wird, schließen Sie die DPM-Verwaltungskonsole, und öffnen Sie sie erneut.
3. Wenn das Problem dadurch nicht behoben wird, beenden Sie den DPM-Dienst und den SQL Server-Dienst, und öffnen Sie beide Dienste erneut. (In der Regel wird das Problem durch einen Neustart des DPM-Diensts behoben.) Weitere Informationen finden Sie weiter oben in diesem Kapitel unter „Überprüfen des Status des DPM-Diensts“.

Wenn permanente Datenbankfehler in DPM auftreten, können die Ursachen dafür komplex sein. Für die Diagnose und Behebung dieser Probleme müssen Sie mit dem SQL Server-Administrator zusammenarbeiten. In Tabelle 6.8 sind allgemeine Anleitungen zum Beheben spezifischer Datenbankfehler aufgeführt.

Tabelle 6.8 Datenbankfehler

Fehler	Problembehandlung
Fehler 940: Verbindung zur Datenbank kann aufgrund von schwerwiegendem Datenbankfehler nicht hergestellt werden. Eine Beschädigung der Datenbank selbst ist unwahrscheinlich.	Vergewissern Sie sich, dass die DPM-Instanz von SQL Server (der Dienst MSSQL$Microsoft$DPM$) ausgeführt wird. Suchen Sie anschließend mit der Windows-Ereignisanzeige nach Informationen zu zugehörigen Ereignissen.
Fehler 941: Verbindung zur DPM-Datenbank kann nicht hergestellt werden.	**So beheben Sie Probleme bei Fehlern mit der Datenbankverbindung** 1. Stellen Sie sicher, dass der Dienst MSSQL$Microsoft$DPM$ ausgeführt wird. 2. Beheben Sie vorübergehende Probleme, die möglicherweise durch temporäre Fehler mit der Datenbankverbindung verursacht werden. 3. Überprüfen Sie die ordnungsgemäße Konfiguration von SQL Server. Informationen zum Konfigurieren von SQL Server für die Verwendung mit DPM finden Sie im Kapitel „Installieren von DPM“ (http://go.microsoft.com/fwlink/?linkid=46357) im Planungs- und Bereitstellungshandbuch von DPM 2006. 4. Weitere Informationen zum Beheben von Verbindungsproblemen in SQL Server 2000 finden Sie in Artikel Nr. 827422, „How to troubleshoot connectivity issues in SQL Server 2000“ (http://go.microsoft.com/fwlink/?LinkId=51138, in englischer Sprache), in der Microsoft Knowledge Base.

Wenn die Integrität einer Datenbank fraglich ist, wenden Sie sich an den SQL Server-Administrator. Möglicherweise müssen Sie die Datenbank in SQL Server mithilfe von Sicherungsmedien reparieren oder wiederherstellen. Informieren Sie stets den Administrator, wenn dieser Fehler auftritt. Suchen Sie im Windows-Ereignisprotokoll nach SQL Server- oder Medienfehlern. Möglicherweise liegt das Problem im Cache anstatt auf dem Datenträger selbst. In diesem Fall wird das Problem durch einen Neustart von SQL Server behoben. In einigen Fällen kann das Wiederherstellen der Datenbank erforderlich sein. **So beheben Sie Probleme mit einer beschädigten Datenbank** 1. Suchen Sie mit der Ereignisanzeige nach E/A-Problemen zum Zeitpunkt der Warnung. E/A-Fehler im Ereignisprotokoll erklären möglicherweise die Ursache der Datenbankbeschädigung. In diesem Fall sollten Sie vor dem Wiederherstellen der Datenbank den Datenträger reparieren oder ersetzen. 2. Führen Sie eine Überprüfung der Datenbank durch, deren Integrität fraglich ist, um das Ausmaß des Datenbankproblems festzustellen. Geben Sie in SQL Query Analyzer den folgenden Befehl ein: **dbcc checkdb** Datenbankname 3. Je nach Art des Problems kann das Reparieren oder Wiederherstellen der Datenbank erforderlich sein. Verschiedene Probleme, z. B. Probleme beim Indizieren und Zwischenspeichern, können durch Reparieren der Datenbank oder einen Neustart von SQL Server behoben werden. Legen Sie zusammen mit dem SQL Server-Administrator die beste Vorgehensweise fest.	

Fehler 943: Die Verbindung zur DPM-Datenbank kann nicht hergestellt werden, da sich die Datenbank in einem inkonsistenten Zustand befindet.	Wenn DPM eine Datenbank in einem inkonsistenten Zustand feststellt, wird sich dieses Problem wahrscheinlich nicht von selbst beheben. Wenden Sie sich an den Microsoft-Produktsupport, um Unterstützung zur Behebung des Problems zu erhalten. Weitere Informationen finden Sie unter Microsoft Hilfe und Support (http://go.microsoft.com/fwlink/?linkid=45276, in englischer Sprache).

Fehler 944: Datenbankvorgang fehlgeschlagen.	• Wenn Zeitüberschreitungen des Clients und allgemeine Netzwerkfehler auftreten, die möglicherweise darauf zurückzuführen sind, dass SQL Server die Anzahl der Abfragen nicht verarbeiten kann, ändern Sie die Schutzzeitpläne für die Schutzgruppen, um die Schutzaufträge zu staffeln. Weitere Informationen finden Sie unter „How to modify protection options“ (http://go.microsoft.com/fwlink/?linkid=52008, in englischer Sprache) in der DPM-Hilfe. • Ein häufiges Auftreten von Zeitüberschreitungen des Clients kann auf eine starke Fragmentierung des Volume hinweisen, auf dem die Datenbankdateien und Transaktionsprotokolle gespeichert sind. Defragmentieren Sie, sofern erforderlich, das Volume mithilfe der Datenträgerdefragmentierung. Weitere Informationen finden Sie unter „Disk Defragmenter: Defragment a Volume“ unter Windows Server 2003 Hilfe und Support (in englischer Sprache). • Durch ungenügenden Speicherplatz für eine SQL Server-Datenbankdatei oder ein Transaktionsprotokoll wird in SQL Server je nach Ausmaß des Speichermangels eine Warnung oder ein Fehler ausgegeben. Bei einem Transaktionsprotokollüberlauf wird der DPM-Dienst wahrscheinlich beendet, nachdem mehrere Zugriffsversuche auf die Datenbank fehlgeschlagen sind. So beheben Sie Probleme bei unzureichendem Speicherplatz für Datenbanken oder Transaktionsprotokolle a. Suchen Sie mit der Windows-Ereignisanzeige zusätzliche Informationen zu diesem Problem. b. Suchen Sie mit SQL Query Analyzer Informationen zur Größe der Datenbank und Speicherplatzauslastung durch Transaktionsprotokolle. Geben Sie die folgenden Befehle ein: **sp_helpdb** – Meldet die Größe der einzelnen Datenbankdateien. **dbcc sqlperf (logspace)** – Meldet die aktuelle Größen der Transaktionsprotokolle. Kapitel 6 Problembehandlung Verkleinern Sie die Datenbank und Transaktionsprotokolle. Geben Sie in SQL Query Analyzer den folgenden Befehl ein: **dbcc shrinkfile (databasenamelogdat)** –Verkleinert die Datenbank und Transaktionsprotokolle.

Fehler 945: Verbindung zur DPM-Datenbank kann aufgrund eines allgemeinen Datenbankfehlers nicht hergestellt werden.	Stellen Sie bei allgemeinen Datenbankfehlern sicher, dass der Dienst MSSQL$Microsoft$DPM$ auf dem DPM-Server ausgeführt wird. Suchen Sie anschließend mit der Windows-Ereignisanzeige nach Informationen zu zugehörigen Ereignissen. Vergewissern Sie sich bei einem neuen DPM-Server, dass SQL Server ordnungsgemäß konfiguriert ist. **So beheben Sie Probleme bei allgemeinen Datenbankfehlern** 1. Stellen Sie sicher, dass der SQL Server-Dienst (MSSQL$Microsoft$DPM$) ausgeführt wird. 2. Beheben Sie vorübergehende Probleme, die möglicherweise durch temporäre Fehler mit der Datenbankverbindung verursacht werden. 3. Überprüfen Sie die ordnungsgemäße Konfiguration von SQL Server. Informationen zum Konfigurieren von SQL Server für die Verwendung mit DPM finden Sie im Kapitel „Installieren von DPM“ (http://go.microsoft.com/fwlink/?linkid=46357) im Planungs- und Bereitstellungshandbuch von DPM 2006. 4. Wenn weiterhin allgemeine Datenbankfehler auftreten, wenden Sie sich an den Microsoft-Produktsupport, um Informationen zur Problembehandlung zu erhalten. Weitere Informationen finden Sie unter Microsoft Hilfe und Support (http://go.microsoft.com/fwlink/?linkid=45276, in englischer Sprache).

Weitere Ressourcen für die Datenbankproblembehandlung

In folgenden Quellen finden Sie Informationen zu diesen Themen:

- Informationen zum Konfigurieren von SQL Server für die Verwendung mit DPM finden Sie im Kapitel „Installieren von DPM“ (http://go.microsoft.com/fwlink/?linkid=46357) im Planungs- und Bereitstellungshandbuch von DPM 2006.
- Informationen zum Sichern und Wiederherstellen der für DPM erforderlichen Datenbanken finden Sie in diesem Handbuch im Kapitel „Archivieren und Wiederherstellen von Daten“.
- Informationen zur gespeicherten Systemprozedur sp_helpdb für SQL Server finden Sie unter dem entsprechenden Eintrag unter „Transact-SQL Reference“ (http://go.microsoft.com/fwlink/?linkid=51140, in englischer Sprache).
- Informationen zu den Datenbankkonsolenbefehlen **dbcc sqlperf** und **dbcc shrinkfile** für SQL Server 2000 finden Sie unter dem Eintrag „DBCC“ in "Transact-SQL Reference" (http://go.microsoft.com/fwlink/?LinkId=52528, in englischer Sprache).

- Informationen zum Identifizieren von Problemen mithilfe von Ereignisprotokollen finden Sie unter „Checking event logs: Common administrative tasks“ unter Microsoft Windows Server 2003 Hilfe und Support (in englischer Sprache).
- Prüfen Sie bei Problemen mit SQL Server mithilfe von SQL Server Enterprise Manager die aktuellen Aktivitäten, Sperren und Prozesse in SQL Server. Weitere Informationen finden Sie unter „Monitoring with SQL Enterprise Manager“ in SQL Server 2000 Books Online (http://go.microsoft.com/fwlink/?linkid=51137, in englischer Sprache).
- Informationen zum Konfigurieren und Warten physischer Speicherkomponenten in SQL Server 2000 zum Erfüllen der Kapazitäts-, Durchsatz- und Leistungsanforderungen finden Sie unter „Capacity and Storage Management“ im Microsoft SQL Server 2000-Benutzerhandbuch (http://go.microsoft.com/fwlink/?LinkId=51142, in englischer Sprache).

Behandeln von Problemen beim Archivieren und Wiederherstellen von DPM

Dieser Abschnitt enthält Informationen zur Behandlung von folgenden Archivierungs- und Wiederherstellungsproblemen in DPM:

- DpmBackup und DPM Writer
- FsPathMerge
- DpmPathMerge

Eine Anleitung für das Verwenden von DpmBackup, FsPathMerge und DpmPathMerge finden Sie im Kapitel „Archivieren und Wiederherstellen von Daten“ in diesem Handbuch (http://go.microsoft.com/fwlink/?LinkId=46368).

Behandeln von Problemen mit DpmBackup und DPM Writer

Wenn ein Problem mit DpmBackup auftritt, warten Sie zehn Minuten, und führen Sie dann DpmBackup (bis zu dreimal) erneut aus. Wenn DpmBackup immer noch nicht erfolgreich ausgeführt werden kann, finden Sie in Tabelle 6.9 die zur Lösung der jeweiligen Fehlerbedingung erforderlichen Schritte.

Der Abschluss von DpmBackup kann aufgrund von Problemen mit der Kommunikation, dem Zugriff oder dem Speicherplatz fehlschlagen. Einige dieser Probleme sind vorübergehend und beheben sich selbst.

Tabelle 6.9 Behebung von DpmBackup- und DPM Writer-Fehlern

Fehlermeldung	Mögliche Ursachen	Problembehandlung
Fehler 4200: Es konnte kein Kontakt zu DPM Writer hergestellt werden. Stellen Sie sicher, dass Data Protection Manager installiert ist und dass der DPM Writer-Dienst ausgeführt wird.	Dieser Fehler kann auftreten, wenn DPM Writer nicht in VSS registriert und als im System verfügbare Speichersoftware aufgeführt ist.	1. Starten Sie DPM Writer mithilfe des Snap-Ins **Dienste** neu. 2. Starten Sie den Volumeschattenkopie-Dienst mithilfe des MMC-Snap-Ins **Dienste** neu. 3. Führen Sie DpmBackup erneut aus. 4. Wenn das Problem mit diesen Schritten nicht behoben werden kann, suchen Sie im Ereignisprotokoll nach DPM Writer-Fehlern.
Fehler 4201: Der Sicherungsvorgang wurde nicht erfolgreich abgeschlossen. Einige Sicherungsschatten-kopien konnten nicht erstellt werden. Führen Sie den Sicherungsvorgang erneut durch.	Dieser Fehler kann auftreten, wenn die Schattenkopien nicht im Ordner **Schattenkopie** bereitgestellt oder nicht erfolgreich erstellt werden. Diese Fehlermeldung wird auch angezeigt, wenn DpmBackup nicht erfolgreich abgeschlossen wurde und keine andere Fehlermeldung gilt.	Wenn in diesem Ordner Dateien manuell erstellt wurden, löschen Sie diese aus dem Ordner **Schattenkopie** der fehlschlagenden Volumes, und führen Sie DpmBackup erneut aus. Wenn DpmBackup immer noch nicht erfolgreich abgeschlossen werden kann, führen Sie die folgenden Schritte durch: 1. Starten Sie DPM Writer mithilfe des MMC-Snap-Ins **Dienste** neu. 2. Starten Sie den Volumeschattenkopie-Dienst mithilfe des MMC-Snap-Ins **Dienste** neu. 3. Führen Sie DpmBackup erneut aus. 4. Wenn das Problem mit diesen Schritten nicht behoben werden kann, suchen Sie im Ereignisprotokoll nach DpmBackup-Fehlern.
Fehler 4202: Der Sicherungsvorgang ist fehlgeschlagen. Mindestens eines der Replikat-Volumes verfügt nicht über ausreichend Festplattenspeicher für die Sicherungsschatten-kopie.	Dieser Fehler tritt auf, wenn in einem Replikatvolume im Speicherpool nicht genügend Speicherplatz vorhanden ist.	1. Ermitteln Sie, welches Volume fehlgeschlagen ist, indem Sie die Ausgabe des Befehls DpmBackup überprüfen. 2. Erhöhen Sie den auf diesem Volume verfügbaren Speicherplatz. 3. Führen Sie DpmBackup erneut aus.

Fehler 4204: Der Sicherungsvorgang ist fehlgeschlagen. DpmBackup konnte die bereits zuvor erstellten Sicherungsschatten-kopien nicht löschen.	Beim Ausführen von DpmBackup werden bei vorherigen Sicherungsvorgängen von DpmBackup erstellte Schattenkopien gelöscht. Anschließend werden im gleichen Pfad neue Schattenkopien bereitgestellt. Dieser Fehler tritt auf, wenn die bereits vorhandenen Schattenkopien nicht erfolgreich gelöscht werden.	1. Stellen Sie sicher, dass keine Änderungen an der Volume- oder Festplattenkonfiguration durch Benutzer vorgenommen wurden. 2. Starten Sie den Volumeschattenkopie-Dienst mithilfe des MMC-Snap-Ins **Dienste** neu. 3. Überprüfen Sie den Status der zu sichernden Festplatte oder des Volume. 4. Führen Sie DpmBackup erneut aus.
Fehler 4205: DpmBackup konnte die DPM- oder DPM Report-Datenbanken nicht sichern.	DPM verwendet zur Sicherung der DPM- und Berichtsdatenbanken SQL Distributed Management Objects (SQL-DMO). Dieser Fehler tritt aufgrund eines Problems mit der SQL-DMO-Sicherung auf.	1. Überprüfen Sie das Anwendungsereignisprotokoll auf SQL Server-Meldungen. 2. Überprüfen Sie das Vorhandensein und die Funktionstüchtigkeit der Datenbanken auf dem SQL Server-Server mithilfe des MMC-Snap-Ins **SQL Enterprise-Manager**. 3. Stellen Sie sicher, dass die Berechtigungen auf der Datenbank und für den Datenbanksicherungsordner nicht geändert wurden. 4. Wenn das Problem mit diesen Schritten nicht behoben werden kann, starten Sie die SQL Server-Dienste neu.
Fehler 4206: DPM Writer konnte keine Verbindung zur angegebenen Datenbank herstellen. Stellen Sie sicher, dass die SQL Server-Dienste mit den entsprechenden Berechtigungen ausgeführt werden.	Dieser Fehler tritt auf, wenn VSS und DPM Writer keine Verbindung über Microsoft SQL Server Desktop Engine (MSDE) Writer zu den DPM- und Berichtdatenbanken herstellen können. Wenn dieser DPM Writer-Fehler beim Ausführen einer anderen Anwendung als DpmBackup auftritt, verwenden Sie als Quelle zur Fehlerbehebung die Dokumentation der entsprechenden Anwendung.	1. Überprüfen Sie das Vorhandensein und die Funktionstüchtigkeit der Datenbanken auf dem SQL Server-Server mithilfe des MMC-Snap-Ins **SQL Server Enterprise Manager**. 2. Starten Sie die SQL Server-Dienste neu.

Fehler 4207: DPM Writer konnte die angegebene Datenbank nicht abfragen. Stellen Sie sicher, dass die SQL Server-Dienste mit den entsprechenden Berechtigungen ausgeführt werden.	Dieser Fehler tritt aufgrund einer SQL Server-Ausnahme auf.	1. Überprüfen Sie das Anwendungsereignisprotokoll auf SQL Server-Meldungen. 2. Überprüfen Sie das Vorhandensein und die Funktionstüchtigkeit der Datenbanken auf dem SQL Server-Server mithilfe des MMC-Snap-Ins **SQL Server Enterprise Manager**. 3. Starten Sie die SQL Server-Dienste neu.
Fehler 4208: DPM Writer konnte nicht auf die Registrierung zugreifen. Stellen Sie sicher, dass Data Protection Manager ordnungsgemäß installiert wurde.	Dieser Fehler tritt auf, wenn DPM-Registrierungs-schlüssel nicht ordnungsgemäß geändert wurden oder beschädigt sind.	• Wenn Ihnen die Änderungen an der Registrierung bekannt sind, setzen Sie diese in den vorherigen Zustand zurück. • Es kann versucht werden, dieses Problem zu beheben, indem Sie DPM unter Verwendung der Option zum Beibehalten der Daten deinstallieren und anschließend dieselbe DPM-Version am selben Speicherplatz erneut installieren. • Wenn Ihnen keine Änderungen an der Registrierung bekannt sind, oder diese nicht wiederhergestellt werden kann, wenden Sie sich an Microsoft Hilfe und Support (http://go.microsoft.com/fwlink/?linkid=45276, in englischer Sprache).
Fehler 4209: Es ist ein interner DPM Writer-Fehler aufgetreten. Starten Sie den DPM Writer-Dienst neu, und führen Sie anschließend erneut einen Sicherungsvorgang durch.	Dieser Fehler kann verschiedene Ursachen haben.	• Starten Sie DPM Writer mithilfe des MMC-Snap-Ins **Dienste** neu, und führen Sie anschließend DpmBackup erneut aus. • Starten Sie den DPM-Server neu, und führen Sie anschließend DpmBackup erneut aus. • Überprüfen Sie die Anwendungs- und Systemereignisprotokolle auf Informationen zu diesem Fehler. • Wenden Sie sich an Microsoft Hilfe und Support (http://go.microsoft.com/fwlink/?linkid=45276, in englischer Sprache).

Fehler 4210: Es ist ein interner DpmBackup-Fehler aufgetreten. Führen Sie den Sicherungsvorgang erneut durch.	Dieser Fehler kann verschiedene Ursachen haben.	• Starten Sie DPM Writer mithilfe des MMC-Snap-Ins **Dienste** neu, und führen Sie anschließend DpmBackup erneut aus. • Starten Sie den DPM-Server neu, und führen Sie anschließend DpmBackup erneut aus. • Überprüfen Sie die Anwendungs- und Systemereignisprotokolle auf Informationen zu diesem Fehler. • Wenden Sie sich an Microsoft Hilfe und Support (http://go.microsoft.com/fwlink/?linkid=45276, in englischer Sprache).
Fehler 4211: Sie verfügen nicht über die erforderlichen Berechtigungen, um diesen Vorgang durchzuführen.	Dieser Fehler tritt auf, wenn DpmBackup über ein Konto ausgeführt wird, das nicht über das Benutzerrecht zur Sicherung von Dateien und Verzeichnissen verfügt.	1. Stellen Sie sicher, dass das für das Ausführen von DpmBackup verwendete Konto ein Mitglied der Sicherungs-Operatoren- oder Administratorengruppe ist. 2. Stellen Sie im Snap-In **Lokale Sicherheitsrichtlinie** sicher, dass die Sicherungs-Operatoren- und Administratorengruppen über das Recht zum Sichern von Dateien und Verzeichnissen verfügen. Dieses Benutzerrecht befindet sich unter **Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten**. 3. Starten Sie DPM Writer mithilfe des MMC-Snap-Ins **Dienste** neu. 4. Starten Sie den Volumeschattenkopie-Dienst mithilfe des MMC-Snap-Ins **Dienste** neu. 5. Führen Sie DpmBackup erneut aus. 6. Wenn das Problem mit diesen Schritten nicht behoben werden kann, starten Sie DPM-Server neu, und führen Sie anschließend DpmBackup erneut aus. 7. Stellen Sie außerdem sicher, dass die Sicherheitsberechtigungen in der Verzeichnisstruktur **Programme\Microsoft Data Protection Manager** nicht geändert wurden.

Fehler 4213: Der Sicherungsvorgang ist fehlgeschlagen. DpmBackup konnte den DPM Writer-Dienst nicht starten.	Dieser Fehler kann auftreten, wenn: • das Konto, unter dem DPM Writer ausgeführt wird, geändert wurde oder ein falsches Konto angegeben wurde. DPM Writer das Konto Microsoft$DpmWriter$ verwendet. • das Kennwort für das Konto, unter dem DPM Writer ausgeführt wird, geändert wurde, oder ein falsches Kennwort angegeben wurde. • der Dienststeuerungs-Manager DPM Writer nicht starten kann, da Berechtigungen geändert oder entfernt wurden. • der DPM Writer-Dienst gelöscht wurde.	1. Überprüfen Sie die Anwendungs- und Systemereignisprotokolle auf Ursachen für das Fehlschlagen des Starten des Diensts. 2. Starten Sie DPM Writer mithilfe des MMC-Snap-Ins **Dienste**.
Fehler 4214: DpmBackup konnte den DPM Writer-Dienst nicht anhalten. Halten Sie den Dienst mithilfe des MMC-Snap-Ins **Dienste** manuell an.	Dieser Fehler kann auftreten, wenn: • der DPM Writer-Dienst mit einem Sicherungs-vorgang ausgelastet ist. • die DpmBackup-Berechtigungen geändert wurden, sodass keine Berechtigung für das Anhalten des Diensts mehr vorhanden ist.	1. Überprüfen Sie die Anwendungs- und Systemereignisprotokolle auf Ursachen für das Fehlschlagen des Anhaltens des Diensts. 2. Halten Sie DPM Writer mithilfe des MMC-Snap-Ins **Dienste** an.

Behandeln von Problemen mit FsPathMerge

Zur Problembehandlung mit FsPathMerge müssen Ihnen die beim Ausführen dieses Befehls auftretenden Schritte bekannt sein.

Wenn auf dem Datei- oder DPM-Server Replikatdaten von Band wiederhergestellt werden, beinhaltet der Befehl FsPathMerge den Pfad des geschützten Ordners (Zielpfad) und des Ordners, der die wiederhergestellten Daten beinhaltet (wiederhergestellter Pfad). In Tabelle 6.10 ist der Prozess dargestellt, anhand dessen FsPathMerge die richtigen Pfadinformationen für die wiederhergestellten Daten wiederherstellt, die hier als Beispiel mithilfe von DpmBackup archiviert wurden. Die über FsPathMerge in den einzelnen Schritten vorgenommenen Dateinamenänderungen sind fett dargestellt.

Tabelle 6.10 Funktionsweise von FsPathMerge: Beispiel

Schritt	Name des Zielpfads	Name des wiederhergestellten Pfads
Anfangspfade bei der Datenwiederherstellung:	C:\Sales	C:\Sales\Programme\Microsoft Data Protection Manager\DPM\\Volumes\ShadowCopy\FS01\C-8d2a01f3-4b01-11d9-b735-806e6f6e6963\ReplicaDir\Sales\Data
1. Benennen Sie den wiederhergestellten Pfad in das Ziel **Path_temp** um.	C:\Sales	C:**Salestemp**
2. Benennen Sie den Zielpfad in das Ziel **Path_old** um.	C:**Salesold**	C:\Sales_temp
3. Benennen Sie das Ziel **Path_temp** in den Zielpfad um.	C:\Sales_old	C:**Sales**
4. Löschen Sie das Ziel **Path_old**.		C:\Sales

Nun verfügen die wiederhergestellten Daten über die richtigen Pfadinformationen.

In Tabelle 6.11 wird beschrieben, wie bei der Pfadzusammenführung auftretende Fehler behoben werden können. Um die fehlgeschlagene FsPathMerge-Aktion zu ermitteln, untersuchen Sie die vorhandenen Ordner unter dem Zielpfadnamen und dem Namen für den wiederhergestellten Pfad. Diese Namen wurden im Befehl FsPathmerge angegeben. Wenn zum Beispiel die Ordner **C:\Sales_old** und **C:\Sales_temp** (siehe Tabelle 6.10) erstellt wurden, der Ordner **C:\Sales** jedoch fehlt, steht fest, dass FsPathMerge in Schritt 3 fehlgeschlagen ist.

Tabelle 6.11 Behandeln von Problemen, die während des FsPathMerge-Prozesses auftreten

Interne FsPathMerge-Aktion	Führen Sie beim Fehlschlagen der Aktion folgende Schritte durch:
Benennen Sie den wiederhergestellten Pfad in das Ziel **Path_temp** um.	1. Löschen Sie das vorhandene Ziel **Path_temp** manuell. 2. Stellen Sie die Daten erneut von Band wieder her. 3. Führen Sie FsPathMerge erneut aus. **Hinweis** Wenn der Pfad mehr als 255 Zeichen enthält, kann dieser nicht manuell gelöscht werden. Führen Sie stattdessen FsPathMerge mit dem Schalter **–D** aus.
Benennen Sie den Zielpfad in das Ziel **Path_old** um.	1. Löschen Sie den Zielpfad und das Ziel **Path_old**, sofern vorhanden, manuell. 2. Benennen Sie das Ziel **Path_temp** manuell in den Zielpfad um. 3. Dadurch wird die Datenwiederherstellung abgeschlossen.
Benennen Sie das Ziel **Path_temp** in den Zielpfad um.	1. Löschen Sie das Ziel **Path_old** manuell. 2. Benennen Sie das Ziel **Path_temp** manuell in den Zielpfad um. 3. Dadurch wird die Datenwiederherstellung abgeschlossen.
Löschen Sie das Ziel **Path_old**.	Löschen Sie das Ziel **Path_old** manuell. Dadurch wird die Datenwiederherstellung abgeschlossen.

In Tabelle 6.12 wird beschrieben, wie Sie auf bestimmte Fehlermeldungen reagieren sollten, die Sie bei der Ausführung von FsPathMerge möglicherweise empfangen.

Tabelle 6.12 Reagieren auf FsPathMerge-Fehlermeldungen

Fehlermeldung	Mögliche Ursachen	Mögliche Lösungen
Sie verfügen nicht über die erforderlichen Berechtigungen, um diesen Vorgang durchzuführen.	Dieser Fehler tritt beim Ausführen von FsPathMerge auf, wenn ein Konto verwendet wird, das nicht über das Benutzerrecht für die Sicherung von Dateien und Verzeichnissen verfügt.	1. Stellen Sie sicher, dass das für das Ausführen von FsPathMerge verwendete Konto ein Mitglied der Sicherungs-Operatoren- oder Administratorengruppe ist. 2. Stellen Sie im Snap-In **Lokale Sicherheitsrichtlinie** sicher, dass die Sicherungs-Operatoren- und Administratorengruppen über das Recht zum Sichern von Dateien und Verzeichnissen verfügen. Dieses Benutzerrecht befindet sich unter **Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten**. 3. Führen Sie FsPathMerge erneut aus. 4. Wenn das Problem mit diesen Schritten nicht behoben werden kann, starten Sie den Dateiserver neu, und führen Sie anschließend FsPathMerge erneut aus.
Es ist ein interner FsPathMerge-Fehler aufgetreten. Führen Sie den Vorgang erneut durch.	Dieser Fehler kann verschiedene Ursachen haben. Er kann auftreten, wenn FsPathMerge mit dem Schalter **–D** ausgeführt wird und der Zielpfad nicht vorhanden ist.	• Stellen Sie sicher, dass keine Benutzer oder Anwendungen auf die Dateien zugreifen, die Sie wiederherstellen, und führen Sie anschließend FsPathMerge erneut durch. • Stellen Sie sicher, dass Sie über die erforderlichen Zugriffsrechte für das Löschen der ursprünglichen Inhalte des Zielpfads und für das Verschieben der Inhalte zum wiederhergestellten Pfad verfügen. • Stellen Sie sicher, dass keine der Dateien oder Verzeichnisse in der Hierarchie gesperrt oder schreibgeschützt sind, und führen Sie FsPathMerge erneut aus.

Hinweis

Für die durch FsPathMerge generierten Fehler werden keine DPM-Fehlermeldungsnummern angezeigt.

Behandeln von Problemen mit DpmPathMerge

Um Fehler mit DpmPathMerge zu beheben, müssen Ihnen die beim Ausführen dieses Befehls auftretenden Schritte bekannt sein.

Wenn auf dem DPM-Server Replikatdaten von Band wiederhergestellt werden, beinhaltet das Volume den Pfad des neu zugeordneten Replikats (Replikatpfad) und des Ordners, der die wiederhergestellten Daten enthält (wiederhergestellter Pfad). In Tabelle 6.13 ist der Prozess dargestellt, anhand dessen DpmPathMerge die richtigen Pfadinformationen für Daten wiederherstellt, die mithilfe von DpmBackup archiviert wurden. Die über DpmPathMerge in den einzelnen Schritten vorgenommenen Änderungen sind fett dargestellt.

Table 6.13 Funktionsweise von DpmPathMerge

Schritt	Name des Replikatpfads	Name des wiederhergestellten Pfads
Anfangspfade bei der Datenwiederherstellung:	C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb\ReplicaDir\ProtectedFolder	C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb\ReplicaDir\Programme\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb\ReplicaDir\ProtectedFolder
1. Benennen Sie den wiederhergestellten Pfad in das Replikat **Path_temp** um.	C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb\ReplicaDir\ProtectedFolder	C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb**ReplicaDirtemp**\Protected Folder
2. Benennen Sie den Replikatpfad in das Replikat **Path_old** um.	C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb**ReplicaDirold**\ProtectedFolder	C:\Sales\Programme\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb\ReplicaDir_temp\ProtectedFolder

3. Benennen Sie das Replikat **Path_temp** in den Replikatpfad um.	C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb\ReplicaDir_old\ProtectedFolder	C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb**ReplicaDir**\ProtectedFolder
4. Löschen Sie das Replikat **Path_old**.		C:\Programme\Microsoft Data Protection Manager\DPM\Volumes\Replica\FS01\C-7fa3a5e6-929c-11d9-a3b7-000c76289bfb\ReplicaDir\ProtectedFolder

Nun verfügen die wiederhergestellten Daten über die richtigen Pfadinformationen.

In Tabelle 6.14 wird beschrieben, wie bei der Pfadzusammenführung auftretende Fehler behoben werden können. Um die fehlgeschlagene DpmPathMerge-Aktion zu ermitteln, untersuchen Sie die vorhandenen Ordner unter dem Zielpfadnamen und dem Namen für den wiederhergestellten Pfad. Diese Namen wurden im Befehl DpmPathmerge angegeben.

Tabelle 6.14 Behandeln von Problemen, die während des DpmPathMerge-Prozesses auftreten

Interne DpmPathMerge-Aktion	Führen Sie beim Fehlschlagen der Aktion folgende Schritte durch:
Benennen Sie den wiederhergestellten Pfad in das Replikat **Path_temp** um.	1. Löschen Sie das vorhandene Replikat **Path_temp** für das angegebene Replikat manuell. 2. Stellen Sie die Daten erneut von Band wieder her. 3. Führen Sie DpmPathMerge erneut aus.
Benennen Sie den Replikatpfad in das Replikat **Path_old** um.	1. Löschen Sie den Replikatpfad und das Replikat **Path_old**, sofern vorhanden, manuell. 2. Benennen Sie das Replikat **Path_temp** manuell in den Replikatpfad um. 3. Dadurch wird die Replikatwiederherstellung abgeschlossen.
Benennen Sie das Replikat **Path_temp** in den Replikatpfad um.	1. Löschen Sie das Replikat **Path_old** manuell. 2. Benennen Sie das Replikat **Path_temp** manuell in den Replikatpfad um. 3. Dadurch wird die Replikatwiederherstellung abgeschlossen.
Löschen Sie das Replikat **Path_old**.	Löschen Sie das Replikat **Path_old** manuell. Dadurch wird die Replikatwiederherstellung abgeschlossen.

In Tabelle 6.15 wird beschrieben, wie Sie auf bestimmte Fehlermeldungen reagieren sollten, die Sie bei der Ausführung von DpmPathMerge möglicherweise empfangen.

Tabelle 6.15 Reagieren auf DpmPathMerge-Fehlermeldungen

Fehler	Ursache	Problembehandlung
Fehler 4211: Sie verfügen nicht über die erforderlichen Berechtigungen, um diesen Vorgang durchzuführen.	Dieser Fehler tritt beim Ausführen von DpmPathMerge auf, wenn ein Konto verwendet wird, das nicht über das Benutzerrecht für die Sicherung von Dateien und Verzeichnissen verfügt.	1. Stellen Sie sicher, dass das für das Ausführen von DpmPathMerge verwendete Konto ein Mitglied der Sicherungs-Operatoren- oder Administratorengruppe ist. 2. Stellen Sie im Snap-In **Lokale Sicherheitsrichtlinie** sicher, dass die Sicherungs-Operatoren- und Administratorengruppen über das Recht zum Sichern von Dateien und Verzeichnissen verfügen. Dieses Benutzerrecht befindet sich unter **Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten**. 3. Führen Sie DpmPathMerge erneut aus. 4. Wenn das Problem mit diesen Schritten nicht behoben werden kann, starten Sie den DPM-Server neu, und führen Sie anschließend DpmPathMerge erneut aus.
Fehler 4216: DpmPathMerge konnte die angegebene Datenbank nicht abfragen. Stellen Sie sicher, dass die SQL Server-Dienste mit den entsprechenden Berechtigungen ausgeführt werden.	Dieser Fehler tritt aufgrund einer SQL Server-Ausnahme auf.	1. Überprüfen Sie das Anwendungsereignisprotokoll auf SQL Server-Meldungen. 2. Überprüfen Sie das Vorhandensein und die Funktionstüchtigkeit der SQL Server-Datenbanken mithilfe des MMC-Snap-Ins **SQL Server Enterprise Manager**. 3. Starten Sie die SQL Server-Dienste neu.
Fehler 4217: DpmPathMerge konnte nicht auf die Registrierung zugreifen. Stellen Sie sicher, dass Data Protection Manager ordnungsgemäß installiert wurde.	Dieser Fehler tritt auf, wenn DPM-Registrierungsschlüssel nicht ordnungsgemäß geändert wurden oder beschädigt sind.	• Wenn Ihnen die Änderungen an der Registrierung bekannt sind, setzen Sie diese in den vorherigen Zustand zurück. • Es kann versucht werden, dieses Problem zu beheben, indem Sie DPM unter Verwendung der Option zum Beibehalten der Daten deinstallieren und anschließend dieselbe DPM-Version erneut installieren. • Wenn Ihnen keine Änderungen an der Registrierung bekannt sind, oder diese nicht wiederhergestellt werden kann, wenden Sie sich an Microsoft Help and Support (http://go.microsoft.com/fwlink/?linkid=45276).

Fehler 4218: Es ist ein interner DpmPathMerge-Fehler aufgetreten. Führen Sie die Pfadzusammenführung erneut durch.	Dieser Fehler kann verschiedene Ursachen haben.	• Stellen Sie sicher, dass keine Benutzer oder Anwendungen auf die Dateien zugreifen, die Sie wiederherstellen, und dass der DPM-Datei-Agent-Dienst (msdpmreplicaagent.exe) und der DPM-Dienst (msdpm.exe) auf dem DPM-Server angehalten wurden, und führen Sie anschließend DpmPathMerge erneut aus. • Stellen Sie sicher, dass Sie über die erforderlichen Zugriffsrechte für das Löschen der ursprünglichen Inhalte des Replikatpfads und für das Verschieben der Inhalte zum wiederhergestellten Pfad verfügen. • Stellen Sie sicher, dass keine der Dateien oder Verzeichnisse in der Hierarchie gesperrt oder schreibgeschützt sind, und führen Sie DpmPathMerge erneut aus.
Fehler 4219: DpmPathMerge kann irrelevante Pfadinformationen nicht automatisch löschen, da entweder das Replikat aus einer Sicherung wiederhergestellt wurde, die nicht mit DpmBackup erstellt wurde, oder der GUID des geschützten Volume seit dem Erstellen der Sicherung geändert wurde. Um sicherzustellen, dass dieses Replikat mit den geschützten Daten konsistent ist, führen Sie FsPathMerge aus, um so irrelevante Pfadinformationen manuell aus dem wiederhergestellten Replikat zu löschen.	Dieser Fehler kann auftreten, wenn DpmPathMerge in den folgenden Situationen ausgeführt wird: • Sie stellen ein Replikat wieder her, bei dem die Sicherungs- und Replikatordnerhie-rarchien nicht übereinstimmen und die Sicherungskopie nicht mit DpmBackup erstellt wurde. • Die Sicherungskopie wurde mit DpmBackup erstellt, und der GUID des geschützten Volume wurde seit dem Erstellen der Sicherungskopie geändert.	• Führen Sie FsPathMerge auf dem DPM-Server aus. Weitere Anweisungen finden Sie in diesem Handbuch im Kapitel „Archivieren und Wiederherstellen von Daten“.

ANHANG A

Fehlercodes in Data Protection Manager 2006

DPM-Fehlercodes werden durch einen Status oder eine Aktion erstellt. Es wird eine Meldung angezeigt, die Informationen enthält und den Benutzer auf Probleme hinweist. Gegebenenfalls enthält die Fehlermeldung empfohlene Aktionen.

Einige Fehlermeldungen verweisen Sie an das DPM-Betriebshandbuch. Weitere Informationen zur Fehlerbehebung finden Sie in diesem Handbuch im Kapitel „Fehlerbehebung“.

ANHANG B

Schemaerweiterungen in Data Protection Manager 2006

Das Tool DPMADSchemaExtension führt folgende Aufgaben zur Unterstützung der Endbenutzerwiederherstellung aus:

• Erweitert das Schema

• Erstellt einen Container (MS-ShareMapConfiguration)

• Gewährt dem DPM-Server Berechtigungen zum Ändern der Inhalte des Containers

• Fügt Zuordnungen zwischen Quellenfreigaben und Freigaben aus den Replikaten hinzu

In diesem Anhang werden die Klassen und Attribute beschrieben, die Data Protection Manager (DPM) zur Unterstützung der Endbenutzerwiederherstellung zu Active Directory hinzufügt.

Im Thema „Von DPM hinzugefügte Klassen“ werden die Klassen beschrieben, die zu Active Directory hinzugefügt werden, wenn die Endbenutzerwiederherstellung auf DPM aktiviert ist.

Im Thema „Von DPM hinzugefügte Attribute“ werden die Attribute beschrieben, die zu Active Directory hinzugefügt werden, wenn die Endbenutzerwiederherstellung auf DPM aktiviert ist.

Von DPM hinzugefügte Klassen

Wenn die Endbenutzerwiederherstellung aktiviert ist, fügt DPM die Klasse **ms-SrvShareMapping** zum Verzeichnisdienst Active Directory hinzu. Diese Klasse enthält die Zuordnung vom Dateiserver (und der Freigabe) zum DPM-Server (und die Freigabe).

Vorsicht

Es wird empfohlen, diese Klasse nicht zu ändern.

Die folgende Tabelle enthält eine detaillierte Beschreibung der Klasse **ms-SrvShareMapping**.

Attribut	Wert
objectClass	Top
objectClass	classSchema

instanceType	4
possSuperiors	Container
possSuperiors	organizationalUnit
subClassOf	Top
governsID	1.2.840.113556.1.6.33.1.22
mustContain	ms-backupSrvShare
mustContain	ms-productionSrvShare
rDNAttID	Cn
showInAdvancedViewOnly	TRUE
adminDisplayName	ms-backupSrvShare
lDAPDisplayName	ms-backupSrvShare
adminDescription	Führt Server mit freigegebenen Ressourcen auf.
objectClassCategory	1

Von DPM hinzugefügte Attribute

Wenn die Endbenutzerwiederherstellung aktiviert ist, fügt DPM zwei Attribute zu Active Directory hinzu. In der folgenden Tabelle werden die hinzugefügten Attribute aufgelistet:

Attribut	Beschreibung
ms-BackupSrv-Share	Stellt den Namen der DPM-Freigabe und des DPM-Computers als Zeichenfolgen zur Verfügung.
ms-ProductionSrv-Share	Stellt den Namen der Dateiserverfreigabe und des Dateiservercomputers als Zeichenfolgen zur Verfügung.

ms-BackupSrv-Share

Attribut	Wert
objectClass	Top
objectClass	attributeSchema
attributeID	1.2.840.113556.1.6.33.2.23
attributeSyntax	2.5.5.12
rangeUpper	260
isSingleValued	TRUE

showInAdvancedViewOnly	TRUE
adminDisplayName	ms-BackupSrv-Share
adminDescription	Kennzeichnet einen Server mit freigegebenen Ressourcen.
oMSyntax	64
IDAPDisplayName	ms-backupSrvShare
objectCategory	CN=Attribute-Schema,<SchemaContainerDN>

ms-ProductionSrv-Share

Attribut	Wert
objectClass	Top
objectClass	attributeSchema
attributeID	1.2.840.113556.1.6.33.2.24

attributeSyntax	2.5.5.12
rangeUpper	260
isSingleValued	TRUE
showInAdvancedViewOnly	TRUE
adminDisplayName	ms-ProductionSrv-Share
adminDescription	Kennzeichnet einen Server mit freigegebenen Ressourcen.
oMSyntax	64
IDAPDisplayName	ms-productionSrvShare
objectCategory	CN=Attribute-Schema,<SchemaContainerDN>